REVIEWING THE FAFSA DATA BREACH

HEARING

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

MAY 3, 2017

Serial No. 115–46

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://oversight.house.gov

U.S. GOVERNMENT PUBLISHING OFFICE

28–504 PDF WASHINGTON : 2018

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

Jason Chaffetz, Utah, *Chairman*

John J. Duncan, Jr., Tennessee
Darrell E. Issa, California
Jim Jordan, Ohio
Mark Sanford, South Carolina
Justin Amash, Michigan
Paul A. Gosar, Arizona
Scott DesJarlais, Tennessee
Trey Gowdy, South Carolina
Blake Farenthold, Texas
Virginia Foxx, North Carolina
Thomas Massie, Kentucky
Mark Meadows, North Carolina
Ron DeSantis, Florida
Dennis A. Ross, Florida
Mark Walker, North Carolina
Rod Blum, Iowa
Jody B. Hice, Georgia
Steve Russell, Oklahoma
Glenn Grothman, Wisconsin
Will Hurd, Texas
Gary J. Palmer, Alabama
James Comer, Kentucky
Paul Mitchell, Michigan

Elijah E. Cummings, Maryland, *Ranking Minority Member*
Carolyn B. Maloney, New York
Eleanor Holmes Norton, District of Columbia
Wm. Lacy Clay, Missouri
Stephen F. Lynch, Massachusetts
Jim Cooper, Tennessee
Gerald E. Connolly, Virginia
Robin L. Kelly, Illinois
Brenda L. Lawrence, Michigan
Bonnie Watson Coleman, New Jersey
Stacey E. Plaskett, Virgin Islands
Val Butler Demings, Florida
Raja Krishnamoorthi, Illinois
Jamie Raskin, Maryland
Peter Welch, Vermont
Matt Cartwright, Pennsylvania
Mark DeSaulnier, California
John P. Sarbanes, Maryland

JONATHAN SKLADANY, *Staff Director*
WILLIAM MCKENNA, *General Counsel*
KATIE BAILEY, *Government Operations Subcommittee Staff Director*
TROY STOCK, *Information Technology Subcommittee Staff Director*
SHARON CASEY, *Deputy Chief Clerk*
DAVID RAPALLO, *Minority Staff Director*

CONTENTS

REVIEWING THE FAFSA DATA BREACH

Wednesday, May 3, 2017

HOUSE OF REPRESENTATIVES
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
Washington, D.C.

The committee met, pursuant to call, at 9:30 a.m., in Room 2154, Rayburn House Office Building, Hon. Steve Russell presiding.

Present: Representatives Russell, Duncan, Issa, Jordan, Amash, Gosar, Foxx, Meadows, Ross, Walker, Blum, Hice, Grothman, Hurd, Palmer, Mitchell, Cummings, Maloney, Norton, Clay, Connolly, Kelly, Watson Coleman, Plaskett, Krishnamoorthi, Raskin, Welch, DeSaulnier, and Sarbanes.

Also Present: Representative Scott.

Mr. RUSSELL. Good morning. The Committee on Oversight and Government Reform will come to order. Without objection, the chair is authorized to declare a recess at any time.

The chair notes the presence of our colleague, Congressman Bobby Scott from Virginia, and we appreciate his interest in this topic and welcome your participation today, sir. I ask unanimous consent that Congressman Scott be allowed to fully participate in today's hearing. And without objection, it will be so ordered.

I would also like to ask unanimous consent to enter into the record statements from the following organizations: The National Association of Student Financial Aid Administrators, the National College Access Network, the American Council on Education, and EPIC.

Mr. RUSSELL. Today, we are here to talk about a data breach involving a Department of Education website and an IRS web-based application. Every day, literally, adversaries and criminals conduct an unknown number of sophisticated and devastating cyber attacks against our nation. To get the government ahead of the curve will require even more effort on the part of agency heads and chief information officers as we begin the task of modernizing old, outdated, and insecure Federal technologies and network architectures, but we cannot calibrate our defenses and buy the right security platforms unless we understand the threat. We must be honest and transparent about what risks that we face and what damage is being done. Ignoring the problem or underestimating the threat places our nation and its citizens in danger.

Once again, we find ourselves on the Oversight Committee investigating a data breach. Hackers were trying to file fraudulent tax returns and steal refunds. To accomplish this crime, they turned to the Department of Education's FAFSA or Free Application for Fed-

eral Student Aid, .gov network and the data retrieval tool which was designed to try to aid in financial applications.

To get the one piece of information that they desired that they couldn't buy in the marketplace, they came to the tool: specifically, taxpayers' adjusted gross income data. You need that AGI to authenticate your identity for the IRS and file your tax returns, so all hackers needed to do was go to the dark web, buy a cache of American taxpayer personally identifiable information, use that to get into the FAFSA.gov and the data retrieval tool, and then they had everything that they needed to steal taxpaying citizens' refunds.

This is exactly the kind of hacking scheme that the Federal agencies must be aware of when they make their services available online. If sensitive data can be accessed through an online application, it must be secured with strong authentication measures and appropriately encrypted.

We need to call these events what they are: data breaches and major incidents. Facing the truth is important not only because the incidents ultimately affect tens of thousands if not hundreds of thousands of American taxpayers and probably millions of students applying for student aid, but it also—because without understanding the threats we face, we can't protect ourselves.

It took the Internal Revenue Service almost three months to determine that this was a major data breach incident that required congressional notification FISMA requirements. And the Department is still not calling this a major incident, and I would like to find out—and I am sure my colleagues— why. This is not about wordsmithing. What we call these incidents helps us bring the full weight of the Federal Government to bear on the cyber response, getting help to those that have been impacted and making sure the vulnerabilities are defended.

Cybersecurity is a team sport. A leak at one end of the pipe or the other still creates a leak. Agencies must safeguard their data and make sure it goes where they intend. If we have other organizations, tools, or technologies hooked up to our networks or websites, then we are responsible. It only takes one vulnerability and then everyone who is connected to that vulnerability is at risk.

What is so troubling about this incident is that it was detected through suspicious activity accidentally. The hackers inadvertently targeted an IRS employee. Criminals do make dumb mistakes. But so do agencies. I would like to think our detection and defense abilities are more advanced than mistakes of criminals relying on the dumb mistakes that they make.

We aren't going to win this fight unless we understand the threats that we face, the damage that hackers and enemies are doing to us, and what we as a Congress can do to empower agency heads and CIOs to protect our networks. The first step in fighting back is wearing our mistakes like a badge. We should follow it with some grit and determination to not let it happen to the areas of government that have been entrusted to our charge.

Mr. RUSSELL. And with that, I would like to yield to the ranking member, Mr. Cummings.

Mr. CUMMINGS. Thank you very much, Mr. Chairman.

No matter who may define it, this is a major incident, IRS or Education. I am just letting you know it is a major incident. You can put any kind of definition you want on it but I am telling you it is.

I welcome this hearing today. This hearing is about the data retrieval tool, and that is a valid topic that several other committees are also addressing. And I, too, Mr. Chairman want to thank Representative Scott for joining us today. He is one who has addressed these issues for many, many years, and I thank him.

Now, what nobody seems to be addressing is the unethical, abusive, and predatory actions of student loan companies. Last September, the inspector general issued a report finding that multiple student loan companies, which were supposed to be, supposed to be helping students were actually accessing and changing student logon information as part of predatory schemes to access their accounts, change their regular mail and email addresses, and even intercept correspondence. That is a major, major event.

Specifically, the IG reported that the process for logging onto the Federal Student Aid website was, quote, "being misused by commercial third parties to take over borrowers' accounts," end of quote. In one case the IG warned that a student loan company, and I quote, "changed the mailing address, the phone number, and email address for borrowers so that it would be difficult for the borrowers to be contacted by loan servicers," end of quote.

In another case, the IG found that a company charged borrowers monthly fees to, quote, "put their loans into forbearance with the stated promise of eventually enrolling them in the Public Service Loan Forgiveness or some other debt reduction program even though the borrowers in some cases were not qualified for these programs," end of quote. This is major.

The IG also found that these companies were able to, quote, "intercept all of the borrowers' emails, correspondence, including password resets via email, important email notices, and direct communication from FAFSA or the loan servicer," end of quote.

Less than two weeks ago, on April 20, our committee staff conducted a transcribed interview with the special agent in charge of this investigation at the inspector general's office. This is what he told us. He warned that these companies, and I quote, "were controlling thousands of accounts or creating thousands of accounts and controlling them," end of quote. In other words, the very companies that were supposed to be helping students were actually abusing their trust.

These practices are reprehensible, but the IG reported that it could not prosecute these student loan companies because of technicalities. Apparently, these companies forced students to sign powers of attorney to get loans so the companies presumably could try to argue that they were authorized to engage in these abusive activities. Something is awfully wrong with that picture. It is outrageous that these companies effectively got away with behavior they must have known was wrong—no, not must have known, they knew was wrong.

I am eager to hear from today's witnesses about improvements necessary to hold these student loan companies accountable for engaging in these deceptive and abusive practices.

In addition, as we will hear today, criminals were able to compromise the data retrieval tool, which is used it to link student tax information to financial aid and student loan accounts online. These criminals then use this information to file fraudulent tax returns. It is unacceptable that students have to deal with the abusive practices of predatory loan companies, as well as the increased threats of identity theft.

It is critical that we crackdown on these criminal elements and improve the security of the systems. Congress also needs to support these efforts. Severe budget cuts in recent years have made it more difficult to make critical improvements in information technology. President Trump's budget proposal and staff reduction directives would exacerbate these challenges.

Finally, if we really, really want to protect students from the abuses we are addressing here today, Congress obviously cannot abolish the Department of Education, as some of my colleagues have proposed. We must support and increase our nation's investments in our students. As I often say, our children are the living messages we send to a future we will never see. The question is how will we send them? The question is how will we protect them? And this is that moment. This is our watch.

And with that, Mr. Chairman, I yield back.

Mr. RUSSELL. Thank you.

I will hold the record open for five legislative days for any members who would like to submit a written statement.

We will now recognize our panel of witnesses. I am pleased to welcome Mr. James Runcie, the chief operating officer, Office of the Federal Student Aid, Department of Education; Mr. Jason Gray, chief information officer from the Department of Education; Ms. Silvana Gina Garza, chief information officer of the Internal Revenue Service; the Honorable Kenneth C. Corbin, Commissioner, Wage and Investment Division of the Internal Revenue Service; and Mr. Timothy Camus, the deputy inspector general for investigations, Treasury Inspector General for Tax Administration.

We welcome all of you and thank you for being here this morning.

Pursuant to committee rules, all witnesses will be sworn in before they testify. Would you please rise and raise your right hand?

[Witnesses sworn.]

Mr. RUSSELL. Thank you. Please be seated.

Let the record reflect that the witnesses answered in the affirmative.

In order to allow time for discussion, we would appreciate it if you would please limit your oral testimony to five minutes each. Your entire written statement will be made a part of the record.

And with that, I am pleased to recognize Mr. Runcie for five minutes.

WITNESS STATEMENTS

STATEMENT OF JAMES W. RUNCIE

Mr. RUNCIE. Thank you, Chairman Russell, Ranking Member Cummings, and members of the committee, for the opportunity to join you today. I will discuss the events that led to the data re-

trieval tool, or DRT, being disabled, the plan to securely restored the tool, and the actions we've taken to assist students, parents, borrowers, and schools.

As the largest source of Federal student aid for postsecondary education in the U.S., FSA delivered more than $125 billion in aid to over 13 million students attending more than 6,000 schools last year. FSA is committed to safeguarding taxpayer interests as we provide access to Federal student aid for students and their families.

During my tenure at FSA, we have securely managed the growth of the direct loan portion of the student loan portfolio from 9.2 million recipients and $155 billion to 32 million recipients and approximately $1 trillion. One of the critical resources that has assisted the Department in this growth is the DRT. It first became available in 2010 through the joint efforts of the IRS and FSA and provides FSA's customers an effective way to transfer required IRS tax information.

Each year, about half of the 20 million FAFSA filers use the DRT and another 4.5 million borrowers use the tool for the income-driven or IDR plans. In total, over 55 million FAFSA and IDR applications have successfully utilized the DRT since inception. Using the DRT has saved millions of hours of applicants' time, reduced improper payments by billions of dollars, and lowered the verification hurdle for schools and their dedicated staff of financial aid professionals.

Following a broader IRS security review last year, the agency contacted FSA about a potential DRT vulnerability. The joint goal of the IRS and FSA was to minimize the potential vulnerability without causing a major disruption to our customers. We agreed to keep the DRT operational while increasing the monitoring of the tool for suspicious activity.

The IRS and FSA have evaluated many solutions that could be integrated with both applications and would increase the protection of taxpayer information. Many solutions did not meet the required security and privacy threshold or resulted in too many applicants being unable to access Federal Student Aid.

In February, we agreed to develop and implement an encryption solution. This solution would be employed for the 2018–19 award year beginning October 1, 2017. The IRS and FSA also agree that we would continue to monitor the applications for the current award years and still allow for DRT use.

On March 3, the IRS alerted FSA of suspicious activity related to the DRT and suspended its use. The suspicious activity involved bad actors who illegally obtained personal information elsewhere and began filling out FAFSAs in order to access taxpayer information from the IRS through the DRT. This information could then be used to file fraudulent tax returns.

I want to reiterate that we have no evidence that any personal information from the Department systems were accessed. However, with evidence that criminals were starting to exploit the potential vulnerability of the DRT using the tool was no longer an option. The solution to bring back the DRT allows tax information to be electronically transferred, but it will encrypt the information and hide it from applicants' view.

For the DRT—for the IDR application, we are targeting the end of May to have the DRT functionality available to applicants. For the FAFSA we are scheduled to meet the October 1st timing for the '18-'19 award year launch. Due to benefit and risk considerations, the current award year of '17-'18 will not have the DRT available for the remainder of the award year.

Consequently, we are reminding students, parents, and borrowers that they can still apply for aid and repayment plans without the DRT. Our ongoing efforts involve utilizing all of our communications resources, digital properties and vendors, and also leveraging the financial aid community. The Department also issued a communication to schools extending flexibilities regarding verification procedures.

I appreciate the opportunity to provide you with this information, and I welcome any questions you may have here today. Thank you.

[Prepared statement of Mr. Runcie follows:]

Written Testimony
James W. Runcie
Chief Operating Officer
Federal Student Aid
U.S. Department of Education

"Examining the Cybersecurity Incident that Affected the IRS Data Retrieval Tool"
Before the U.S. House of Representatives Committee on Oversight and Government Reform

May 3, 2017

Thank you, Chairman Chaffetz, Ranking Member Cummings, and members of the Committee, for the opportunity to join you today. I will discuss the events that led up to the security incident that precipitated the Internal Revenue Service (IRS) disabling the Data Retrieval Tool (DRT) on March 3, 2017. I also will discuss the plan the U.S. Department of Education (the Department) office of Federal Student Aid (FSA) and the IRS have to restore DRT functionality, as well as actions FSA has taken to assist impacted students, parents, borrowers, and postsecondary institutions.

FSA remains the largest source of Federal student aid for postsecondary education in the United States. In Fiscal Year 2016, FSA delivered nearly $125.7 billion in aid to more than 13 million students attending more than 6,000 postsecondary institutions. In response to legislative, regulatory, and policy changes, FSA has successfully implemented a number of major modifications to our operating environment. One of these developments is the implementation of the DRT, which first became available in 2010.

Background about the DRT

Section 6103 of the Internal Revenue Code/USC restricts the sharing of taxpayer information without their explicit consent. The DRT is a solution the IRS and the Department developed to fit the legal constraints around sharing tax information without explicit consent. The DRT is accessed via the *Free Application for Federal Student Aid* (FAFSA®) where the applicant can explicitly consent to receive their tax data and then electronically transfer that data into the FAFSA application. In essence, the DRT allows the data to electronically flow through the consumer before being transferred into the FAFSA.

The DRT is the result of a collaborative effort between the IRS and FSA, intended to provide students, parents, and borrowers an easy and effective method to access required IRS tax information and transfer that data directly from the IRS into a FAFSA or an income-driven repayment (IDR) plan application. Using the DRT saves time and ensures greater accuracy of applicants' information. Each year, approximately 20 million FAFSA forms are submitted. The most recent data indicate that roughly half of all FAFSA filers use the DRT to transfer their tax information from the IRS, and approximately 4.5 million borrowers use the DRT to transfer their tax information into an IDR plan application.

The existence of the DRT paved the way for two recent FAFSA simplification advancements aimed at reducing barriers to accessing a postsecondary education: the "Early" FAFSA and the use of "prior-prior" year tax information. Traditionally, the FAFSA is available each year on January 1.

Last year, however, FSA launched the 2017–18 FAFSA three months earlier—on October 1, 2016, rather than January 1, 2017—and required applicants to use tax return data from the prior-prior year (2015, not 2016). This change allowed more FAFSA filers to use the DRT, provided students and families with financial aid information earlier to consider in their selection of schools, and allowed applicants to submit a FASFA without having to return to the application in order to correct it after they filed their tax return.

The DRT serves as an important program integrity measure, as well. We know that filers may sometimes incorrectly enter their information into the FAFSA, which may result in improper payments. The DRT essentially eliminates the chances of this type of user error-generated improper payment. It also reduces the need for a secondary program integrity measure. Postsecondary institutions are required to verify certain information from the FAFSA for any applicant who has been selected by the Department for such verification. Nationally, using a risk-assessment regression analysis, the Department selects between 25 and 30 percent of FAFSA filers for verification. Verification requires applicants to provide documentation to their institution—including IRS tax return information—to confirm what was provided by the applicant when completing the FAFSA. For applicants who use the DRT, institutions can rely on the information obtained from the IRS, thereby eliminating the burden associated with manually verifying information students and parents reported. While the DRT was operational, the Department saw decreases in verification rates from the prior year of approximately seven percentage points.

IRS and FSA Joint Efforts to Increase Security of the DRT

In October 2016, the IRS contacted FSA about a potential vulnerability it identified with the DRT as a result of a broader review IRS had undertaken assessing all the ways taxpayers and others interact with IRS' systems. FSA sought to determine the best approach to minimize the vulnerability without causing a major disruption to students, parents, and borrowers. To avoid negative impacts to students, parents, and borrowers, the IRS and FSA agreed to keep the DRT operational while the IRS increased monitoring of the tool for any suspicious activity. The increased monitoring was intended to reduce the risk of exposing tax return information and other personally identifiable information (PII) associated with the DRT without limiting access to the FAFSA and IDR plan applications for a significant segment of students and families.

Since October, the IRS and FSA have evaluated nearly one dozen potential options— capable of being integrated with the FAFSA and IDR plan applications—to increase the protection of taxpayer information on the DRT; options considered include different versions of data masking, slight data modification, higher levels of authentication, or a legislative change to Internal Revenue Code section 6103 that would authorize the Department of Education to securely receive the data directly from the IRS. While we hoped to be able to implement a solution to prevent any disruption to the DRT, evaluating options was crucial in being able to move toward the option we will implement for the 2018–19 FAFSA cycle.

Analyzing and Investigating the Suspicious Activity Related to the DRT

By early March, the IRS identified suspicious activity related to the DRT. On March 3, 2017, the IRS alerted FSA, suspended the use of the DRT, and placed an outage message on the DRT website.

There is no evidence that the malicious actors accessed any personal information from the Department's systems. We are confident that the personal information the Department has on borrowers, students, and parents remains appropriately protected. While the FAFSA was involved, FSA believes this was, in essence, a scheme directed at retrieving tax data from the IRS. Using personal information obtained illegally from other sources—including name, Social Security number, date of birth, address, and tax filing status—malicious actors were able to start filling out FAFSAs. The malicious actors then used the DRT to access taxpayer information from the IRS, including the Adjusted Gross Income, which is necessary to file a fraudulent tax return.

FSA provided the IRS with a preliminary analysis related to the list of potentially impacted taxpayers, which included transactional data from FSA systems, to assist the IRS in reconciling conclusions with its own ongoing analysis. On April 3, 2017, the IRS informed FSA that it was treating the security incident as a "major" incident as defined under the Office of Management and Budget's (OMB) guidance in OMB M-17-12.

The Department continues to review data from the IRS to take necessary administrative action to protect applicant data and taxpayer funds. We are cooperating with the Office of Inspector General and will keep it fully informed as it proceeds with its joint criminal investigation with the Treasury Inspector General for Tax Administration.

Communications to Students, Parents, Borrowers, and Others

FSA recognizes the widespread concern about how the unavailability of the DRT has affected those Americans we serve—particularly those who are from low-income backgrounds or who are first-generation college applicants—and the postsecondary institutions they attend. We remain steadfast in our efforts to fulfill our mission of providing access to higher education for all Americans while protecting sensitive student, parent, and borrower information. We are committed to doing all that we can to help students, parents, and borrowers successfully submit applications by manually providing their tax return information while the DRT is unavailable.

Since the DRT was disabled on March 3, 2017, FSA has provided guidance to the public on multiple platforms indicating that students, parents, and borrowers can still apply for federal student aid and repayment plans. Information also explains how to apply while the tool is unavailable.

The IRS and FSA have released two joint statements—on March 9 and March 30—that inform the public (1) that tax information can be provided manually on both the FAFSA and IDR plan application websites and (2) how to obtain copies of their tax returns, if they are unable to access their own copies. Information about the status of the DRT has been posted to FSA's Information for Financial Aid Professionals (IFAP) website—ifap.ed.gov—which serves as the primary information portal for financial aid professionals, and to StudentAid.gov, FSA's flagship information portal for students, parents, and borrowers.

The March 30 announcement on StudentAid.gov includes detailed instructions about completing a FAFSA without access to the DRT, along with an easy-to-follow table showing which line to reference for specific tax information, depending on which IRS tax form the student or parent filed.

Other ways FSA has shared information to help students, parents, borrowers, and institutions, include:

- Providing FSA customer contact centers with information to explain how students, parents, and borrowers should manually provide tax information for the FAFSA and IDR plan applications. Customer service representatives at the Federal Student Aid Information Center currently are fielding approximately 500 more customer inquiries per day related to the DRT than before the tool was disabled.

- Posting an announcement on its fafsa.gov home page that includes a reminder that information can be entered manually on the application, and FSA links directly to guidance available on the IRS's website that provides students, parents, and borrowers with instructions for obtaining a tax return transcript.

- Using social media applications, Facebook and Twitter, to encourage students, parents, and borrowers to apply for aid by manually providing their tax information. Such messaging via social media has been shared broadly by college access organizations that help support FSA's mission.

- Posting on the Financial Aid Toolkit—a website that provides information for counselors and college access mentors—with links to other related information, making it easy for counselors and mentors to share information with the students they support.

- Emailing approximately 2,000 partner organizations—including counselors, mentors, and financial aid professionals—informing them to plan for the DRT to be unavailable until fall 2017, the beginning of the next FAFSA season.

- Notifying financial aid professionals directly via an Electronic Announcement to schools. The communication advises institutions that the online applications remain operational and that applicants should manually provide financial information from copies of their tax returns.

- Adding language to the IDR plan application informing borrowers that servicers can accept documentation of income by fax or mail, or that they may upload proof of income documents directly and securely through servicers' websites. Contact centers and FSA training officers have been also notified of the additional language.

- Sending a memo to state grant agencies encouraging them to consider providing flexibilities related to application deadlines or other administrative requirements for students and families who may need more time to apply for aid while the DRT is unavailable.

- Issuing a Dear Colleague Letter to postsecondary institutions extending flexibilities institutions may choose to use as part of their verification procedures. These flexibilities begin immediately and apply to both the 2016–17 and 2017–18 FAFSA processing and verification cycles.

At the end of March, FSA provided briefings to staff of several congressional committees, including this committee, the Senate Committee on Homeland Security and Governmental Affairs, the Senate Committee on Finance, the House Committee on Ways and Means, and the Senate Committee on Health, Education, Labor and Pensions. We will continue to be accessible to you and provide

answers to your questions as we work toward making the FAFSA accessible to everyone who wants to go pursue a postsecondary education while protecting sensitive taxpayer data.

The Encryption Solution

In an effort to determine an acceptable solution to a vulnerability related to the DRT, as previously stated, on February 9, 2017, the IRS and FSA agreed to pursue an encryption solution. This solution provides potentially the best balance between securing personal information and access to financial aid under current law and in time for the next federal student aid application cycle, which starts on October 1. The DRT returns 11 taxpayer data elements to the FAFSA and four data elements to the IDR application. The solution will encrypt the taxpayers' information and hide it from applicants' view on the IRS DRT web page, as well as on the FAFSA and IDR plan application web pages. While students, parents, and borrowers will still be able to electronically transfer their own data into a FAFSA or an IDR plan application, taxpayer information will no longer be visible to would-be malicious actors. We acknowledge some filers may have concerns about not being able to see the information they are transferring from the IRS into the FAFSA. We will continue to work with the financial aid community and the IRS to address these concerns.

FSA and the IRS have been working together to expedite the implementation of the encryption solution. The IRS, which had to modify four basic input and output web pages and supporting processes, implemented the majority of the solution in March in a configurable way, which allowed the IRS to turn it on or off separately for the IDR plan application and the FAFSA.

To implement the encryption solution, FSA must re-engineer the IDR plan application and FAFSA application processes. And because process changes to both applications significantly impact other parts of the financial aid ecosystem—students, parents, borrowers, postsecondary institutions, state grant agencies, and servicers, among others—the changes and impacts must be carefully communicated in a thorough, deliberate manner. Obscuring taxpayer information in the FAFSA process will require additional assistance from postsecondary institutions.

Currently, FSA and the IRS are working toward a goal to implement the encryption solution by the end of May or early-June for the IDR plan application. FSA's implementation of the solution for the FAFSA, however, is more complicated.

Each award year involves a separate FAFSA implementation. Presently, there are two active FAFSA cycles:

1. The 2016–17 FAFSA cycle, which began January 1, 2016, and extends until June 30, 2017, when no new applications will be accepted; and
2. The 2017–18 FAFSA cycle, which began October 1, 2016, and extends until June 30, 2018.

The 2018–19 FAFSA cycle will begin October 1, 2017, and will extend until June 30, 2019. The implementation of the 2018–19 FAFSA began in August 2016.

Over the years, FSA has worked to simplify the experience for the FAFSA filer; despite relatively complex program requirements. FSA has implemented improvements to the FAFSA, including skip logic, multiple external interfaces, and hundreds of validation edits in order to assist applicants or to reduce the number of questions posed to applicants, based on their individual circumstances. As would be expected, any time a change is made to the FAFSA process, a significant amount of testing must occur to ensure that the process and supporting web pages operate as intended.

When FSA and the IRS agreed to the encryption solution, FSA had to compress the 2018–19 FAFSA implementation schedule by three months in order to implement the 2018–19 FAFSA by October 1, 2017, as planned. We will implement by that date, and the 2018–19 FAFSA cycle will include the encryption solution.

The earliest possible timeframe to implement the solution for the 2017–18 FAFSA cycle would have been October 1, 2017. By that time, we estimate that 92 percent of the expected 2017–18 FAFSA filers would already have submitted their applications; before the DRT was disabled, approximately 4.7 million 2017–18 FAFSA applicants used the tool.

More critically, in order to implement the solution by October 1 for the 2017–18 FAFSA cycle, FSA would have needed to divert contractor expertise, technical resources, and Federal subject matter experts from the upcoming 2018–19 FAFSA implementation. Striving to make the DRT available to the remaining eight percent of 2017–18 FAFSA filers would have introduced an unacceptable level of risk to the applicants relying on the 2018–19 FAFSA launch. Such a diversion of resources would have significantly increased the likelihood of flaws in the 2018–19 FAFSA implementation or would have caused the 2018–19 FAFSA to be launched after October 1. Diverting resources also could have impacted application processing, resulting in delays in institutions and students accessing Federal loan, grant, and work study funds. Therefore, the DRT will remain unavailable and the encryption solution will not be implemented for the remainder of the 2017–18 FAFSA cycle.

Conclusion

For several months, FSA and the IRS have been working collaboratively to address an identified vulnerability with the DRT, investigate the related security incident, implement short-term solutions, and discuss other options for long-term solutions that ensure that the FAFSA remains accessible to everyone who wants to go to college while protecting sensitive taxpayer data. As FSA works to implement the encryption solution by the end of May or early-June for the IDR plan application and by October 1 for the 2018–19 FAFSA, we also have begun developing comprehensive communications plans for students, parents, borrowers, postsecondary institutions, and others about the solution. We continue to work with the IRS to implement the encryption solution, because we understand that the protection of individuals' personal information is critically important and share the IRS' commitment to make information security a high priority.

I appreciate the opportunity to provide the Committee with an overview of events that precipitated the IRS disabling the DRT, actions FSA has taken to assist impacted students, parents, borrowers, and institutions, and the plan to implement the encryption solution. I welcome any questions you may have today.

Mr. RUSSELL. Thank you.
And the chair now recognizes Mr. Gray for five minutes.

STATEMENT OF JASON K. GRAY

Mr. GRAY. Thank you, Chairman Russell and Ranking Member Cummings and members of the committee. I am Jason Gray, CIO for the U.S. Department of Education, a position I have had the privilege of holding since June of 2016. I appreciate the opportunity to speak with you today on the cybersecurity incident that led to the shutdown of the IRS data retrieval tool.

As the CIO, I embrace and support the Department's mission of promoting student achievement and preparation for global competitiveness, fostering educational excellence, and ensuring equal access by ensuring that we apply information technology effectively, efficiently, and securely. I take this responsibility seriously and understand that this includes the entire Department, including Federal Student Aid and all principal and support offices.

When we became aware that the IRS had confirmed that tax data accessed through the FAFSA link to the DRT may have been used to fraudulently file tax returns, we immediately activated our incident response processes. This involved coordination of Security Operations Center resources to gather forensic data and to gain a better understanding of the incident. We held daily meetings to facilitate communication between the technical staff of my office, Federal Student Aid, and the IRS. Additionally, we reported the incident to the office—to our Office of the Inspector General and to the United States Computer Emergency Readiness Team at Homeland Security.

While the Department systems were involved, this was in essence a scheme directed at retrieving tax data from the IRS. There is no evidence that the malicious actors were able to access any personal information from the Department systems. I am confident that the personal information the Department has on borrowers, students, and parents remains appropriately protected.

I will describe several actions we have taken to further strengthen and enhance our cybersecurity program to protect sensitive data, including PII, that is managed by the Department.

Incident response is a priority for the Department. In 2015, we created an incident response planning workgroup to address cybersecurity incidents and data breach response processes. In 2016, the Department conducted two incident response tabletop exercises that helped us refine our incident response process through the development of lessons learned and identification of actions the Department needed to enhance our overall incident response process.

The Department has implemented a number of technical controls and solutions to detect policy violations, unauthorized changes, and unauthorized access to the Department's primary network. These include a data loss prevention solution, which restricts users from sending emails that contain sensitive PII such as Social Security numbers outside of the Department.

In 2016, the Department also implemented network access control, which prevents connection by any unauthorized device to the network. A third solution, web application firewalls, has been im-

plemented, and we are transitioning web portals and web applications to be protected by those firewalls.

The Department has partnered with DHS on the implementation of automated solutions for continuous diagnostics and mitigation, which will enable us to continuously monitor our network for intrusions and malicious activity. The Department also actively leverages multiple DHS-provided shared security services.

I thank you for the opportunity to discuss the cybersecurity incident that affected the DRT. The Department of Education and the IRS continue working together to continuously enhance the security and privacy protections around this important capability. I am confident that the technical solution currently being worked will achieve this goal. I would be pleased to answer any questions you may have.

[Prepared statement of Mr. Gray follows:]

Written Testimony
Jason K. Gray
Chief Information Officer
U.S. Department of Education

"Examining the Cybersecurity Incident that Affected the IRS Data Retrieval Tool"
Before the U.S. House of Representatives Committee on Oversight and Government Reform

May 3, 2017

Good morning Mr. Chairman, Ranking Member Cummings, and Members of the Committee. I am Jason Gray, Chief Information Officer (CIO) for the U.S. Department of Education ("Department"), a position I have had the privilege of holding since June, 2016.

I appreciate the opportunity to speak with you today on the cybersecurity incident that affected the Internal Revenue Service (IRS) Data Retrieval Tool (DRT), specifically, the operational and cybersecurity decisions before and after the tool was taken offline. As the CIO, I embrace and support the Department's mission of *promoting student achievement and preparation for global competitiveness, fostering educational excellence and ensuring equal access*, by ensuring that we apply information technology (IT) effectively, efficiently, and securely. I take this responsibility seriously, and understand that this includes the entire Department, including Federal Student Aid (FSA) and all principal and support offices.

On March 3, 2017, I became aware that the IRS had confirmed that tax data accessed through the FAFSA DRT may have been used to fraudulently file tax returns. The Department's Security Operations Center (EDSOC) was notified about suspicious behavior on the IRS DRT on March 3, 2017. The DRT is an IRS tool leveraged by the Department's Free Application for Federal Student Aid (FAFSA) by allowing applicants to access required parts of their tax information

electronically for them to insert into their student aid applications. We immediately activated our incident response processes, beginning with actions to understand details of the events that occurred, and to identify appropriate responses. This involved coordination of Security Operations Center resources to gather forensic data and to gain a fuller understanding of the incident. We held daily meetings to facilitate communication between the technical staff of the Office of the Chief Information Officer (OCIO), FSA, and the IRS. Additionally, we reported the incident to our Office of the Inspector General and to the United States – Computer Emergency Readiness Team (US-CERT) at the Department of Homeland Security (DHS) on March 3, 2017, and March 4, 2017, respectively. While the Department's systems were involved, this was, in essence, a scheme directed at retrieving tax data from the IRS. The malicious actors used stolen PII to start FAFSA forms in order to obtain information from the IRS to attempt to file fraudulent tax returns. There is no evidence that the malicious actors were able to access any personal information held on the Department's systems. We are confident that the personal information the Department has on borrowers, students, and parents remains appropriately protected.

This issue, which involved the unlawful use of a Department system by outside parties, underscores the need for the Department to be continually vigilant in the operation and improvement of our cybersecurity capabilities. Toward that end, we have undertaken multiple projects to improve capabilities consistent with Industry Best Practices and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover). The Cybersecurity Framework applies the principles and best practices of risk management to improving the security and resilience of critical infrastructure. I will describe

several actions we have taken to further strengthen and enhance our cybersecurity program to protect sensitive data, including PII that is managed by the Department.

Incident Response

Incident response is a priority for the Department. In 2015 we created an Incident Response Planning Workgroup to address cybersecurity incidents and data breach response processes with separate work streams for communications, breach response planning, and privacy and legal. This group validated the mapping of key network systems, revised agency policies and directives as needed, evaluated and identified necessary amendments to the security clauses in vendor contracts, and developed technical and procedural protocols to guide decision-making in the event of a breach.

In Fiscal Year (FY) 2016, the Department conducted two incident response table-top exercises that helped us refine our incident response process through the development of lessons learned and identification of actions the Department needed to enhance our overall incident response processes. We have taken all actions identified in the two FY 2016 tabletops and plan multiple tabletops in FY 2017 as well.

Additionally, with the publication of the FY 2017 Inspector General Federal Information Security Modernization Act (FISMA) Reporting Metrics, the Department has performed a self-assessment against the Incident Response metric area. The Department is currently working to incorporate additional measures to achieve at least "Level 2" status across our Incident Response

program, to include the consolidation of our Security Operations Center capabilities, processes, and resources.

Internal Technical Controls

The Department has implemented a number of technical controls and solutions to detect policy violations, unauthorized changes, and unauthorized access to the Department's primary network. These include a Data Loss Prevention (DLP) solution, which went live in October of 2016 that restricts users from sending emails that contain sensitive PII, such as social security numbers, outside of the Department. In 2016 the Department also implemented Network Access Control (NAC), which allows for validation of the security posture of all endpoints against standard Department cybersecurity policies, and prevents the connection by any unauthorized device to the network. A third solution, Web Application Firewalls (WAFs), has been implemented and we are transitioning web portals and web applications to be protected by the WAFs.

The Department continues to focus on achieving Federal goals for strong authentication, as 100 percent of privileged users, and over 85 percent of our non-privileged users are required to use their Personal Identity Verification (PIV) card in order to log on to the Department's network.

Outreach and Collaboration with DHS

The Department has partnered with DHS on the implementation of automated solutions for Continuous Diagnostics and Mitigation (CDM), which will enable us to continuously monitor our network for intrusions and malicious activity. The Department also actively leverages DHS-provided shared security services such as EINSTEIN 3A tools for threat analysis and threat

indicators, US-CERT surge support for forensics analysis, and High Value Asset assessments.

The Department is also working in other ways to help ensure only authorized users are accessing the Department's systems and data. The FSA ID—a user-selected username and password—is required for students, parents, and borrowers to authenticate their identity and access their federal student aid information online. The websites that require an FSA ID to log in are fafsa.gov, NSLDS Student Access, StudentAid.gov, StudentLoans.gov, and the Federal Student Aid Feedback System (when a customer chooses to authenticate). Since the implementation of the FSA ID almost two years ago, over 45 million people have successfully created an FSA ID and have used their FSA IDs to log in over 315 million times. Recently the Department announced an additional disclaimer prior to log-in that will warn against unauthorized usage of the FSA ID by third-party for-profit entities. The user must select "Accept" in order to proceed.

While the Department has taken a number of positive steps to prevent the unauthorized access and loss of sensitive data, we recognize that there is still work to be done. The Department has fully embraced and is leveraging the mandates of the Federal Information Technology Acquisition Reform Act (FITARA), which we believe is prudent to continually improve and mature our processes in the realm of overarching IT Security and Governance.

Conclusion

I thank you for the opportunity to discuss the cybersecurity incident that affected the DRT, and the operational and cybersecurity decisions made before and after the tool was taken offline. The Department of Education and the IRS continue working together at all appropriate levels to

significantly improve the security and privacy protections around this important capability. I am confident that the technical solution currently being worked will achieve this goal. I would be pleased to answer any questions you may have.

Mr. RUSSELL. Thank you.
The chair now recognizes Ms. Garza for five minutes.

STATEMENT OF SILVANA GINA GARZA

Ms. GARZA. Chairman Russell, Ranking Member Cummings, and members of the committee, thank you for the opportunity to appear before you today to discuss the cybersecurity incident associated with the Federal Student Aid data retrieval tool, or DRT. I have been a public servant for over 32 years, and I am information technology executive for the last 17. Recently, I became the chief information officer, having served as the deputy CIO for the four years prior.

During this time, I have seen a dramatic change in the number and types of attacks fraudsters and criminal enterprises use to try to get the data we are committed to protecting. As the tactics have changed, the IRS's attitude and approach towards cybersecurity and refund fraud have also changed. We understand that the enemy is ever-changing and that we must stay diligent in continually assessing our risk posture and improving our defenses. We know that we are—we all share the responsibility to ensure that cybersecurity is embedded in every part of our operation.

Stepping into the role of CIO eight months ago, I established two priorities: cybersecurity and delivering a successful filing season. Having been an executive in the Business Operating Division, I appreciate the delicate balance between meeting taxpayer needs with quick and convenient access to online programs and securing our systems.

We did not take lightly the decision to disable the DRT tool. We knew that doing so have the potential to disrupt millions of students applying for Federal financial aid. Even so, I believe we made a sound decision, one which would protect the data of approximately 175 million Americans. This is our highest priority.

I appreciate your decision to conduct a public hearing on the subject, as I believe it is critical that we continue to raise awareness of the widespread cyber and identity theft threats we are facing across the globe today. Every day, thousands of individuals fall victim to identity theft. Government and private sector companies are all being bombarded with cyber attacks. We in the IRS have a front row seat. Every day, the IRS receives and defends on average a million attempts to penetrate our systems. Identity theft continues to be a major threat to our tax administration efforts.

When we first became concerned with the level of authentication protecting the data retrieval tool, we assessed the risk to determine if we should shut down the application. Our practice has been to shut down the application of concern until we have mitigated the risk. In prior situations, no other agency was involved. This situation was different. The Department of Education was highly dependent on the data retrieval tool for the success of its program and to serve its customers. We would not make a decision to shut down the application without engaging the Department of Education in the decision process.

We discussed the need to raise the level of authentication with the Department of Education. Additionally, we discussed the fact that this could be done at either the Department of Education

website or at the point the applicant invokes the DRT tool. The Department of Education needed to have a user-friendly solution in place. This made it undesirable to implement a solution that would cause about 75 percent of applicants to be unable to complete the process. We continued to collaborate with the Department of Ed to find an alternative solution to protect the data.

At that time, there was no evidence of data loss or fraud so we agreed to not shutdown the application while we worked on an acceptable solution. We were always clear that the moment we had evidence of data loss or fraud, we would turn off the data retrieval tool. On March 3, having confirmed an incident of fraud, we turned off the application. Details of the incident and activities leading up to the decision to shut down the application are in the written testimony.

In conclusion, protecting data is our highest priority. This threat is persistent and ever-changing, and the IRS remains diligent and ever watchful. The portion of the funds Congress provided last year to support cybersecurity has helped us implement tools and processes that have enhanced our capabilities, but there will always be more work to be done.

Chairman Russell, Ranking Member Cummings, members of the committee, this concludes my oral testimony. I will be happy to answer your questions.

Mr. RUSSELL. Thank you. The chair now recognizes Mr. Corbin for five minutes.

STATEMENT OF KENNETH C. CORBIN

Mr. CORBIN. Chairman Russell, Ranking Member Cummings, and members of this committee, I am the new commissioner of the IRS's Wage and Investment Division, having started this position at the beginning of the year. My responsibilities include overseeing the processing of tax returns, issuance of refunds, preventing and detecting refund fraud, providing the best possible taxpayer service. Thank you for this opportunity to testify.

My colleague, Ms. Garza, has described the work the IRS is doing in collaboration with the Department of Education to secure the DRT. I will put that in a broader context of how we are working to save at all of our programs where we share taxpayer information. I will also update the committee on our efforts to help taxpayers who may have been affected by the incident earlier this year involving the DRT.

An important focus of the IRS's efforts to protect taxpayer data is the ongoing battle against stolen identity refund fraud. We have made steady progress of the last few years against this threat, but as many colleagues noted, this threat is constantly evolving. To address this challenge, the IRS has worked to increase our ability to monitor, detect, analyze suspicious activity within our systems. Congress helped us by approving $290 million in additional funding in 2016, which included $95 million to improve cybersecurity. We have used a portion of that funding for monitoring equipment and other capabilities that are more sophisticated than we previously had. This is helping us detect unusual activity in our various online tools and applications more quickly.

Despite all this progress we've made, we realize we cannot relax the fight against identity theft. We are finding that, as the IRS enhances return processing filters, catches more fraudulent returns at the time of filing, criminals attempt to become more sophisticated at mimicking taxpayers' identities so they can evade those filters and successfully obtain fraudulent refunds. Therefore, the IRS is working not just to react better and faster but also to stay ahead of the criminals.

In that regard, we've also undertaken a broad effort to review authentication practices for programs where we share taxpayer information and strengthen those practices where necessary. Student aid is an area where we have been concerned about the ability of bad actors to fraudulently obtain taxpayer information. That led us beginning last fall to more closely monitor activity on the DRT and work with the Department of Education to make the DRT more secure. In investigating the incident earlier this year involving the DRT, we found that the data obtained through unauthorized use of the tool was in some cases used to attempt to file false returns.

Our strengthened fraud filters have stopped a significant number of questionable tax returns by filers who access the DRT. We are working to determine whether any of those returns are in fact fraudulent. Our analysis of the suspicious activity involving the DRT found approximately 100,000 individuals may have had their taxpayer information compromised.

While we have indications that a large number of these taxpayers are—in all likelihood did not have any information compromised, in an abundance of caution, we have mailed letters to all of these taxpayers. We wanted to tell them about the possibility of unauthorized activity related to their personal information so they can take steps to secure their data. We also offered them free credit monitoring. Along with notifying these taxpayers, the IRS is marking their accounts to provide additional protection against the possibility that an identity thief could file a false return using their information.

We also recognize that many families trying to apply for student aid have been inconvenienced by the decision to shut off the DRT while we work to improve security for the tool. In the interim, families can still complete the application for student financial aid by manually providing the requested financial information from copies of their return. Although we realize this is not as convenient as using the DRT, we have a responsibility to ensure the DRT and all of our online tools are fully protected from identity thieves.

Chairman Russell, Ranking Member Cummings, and members of this committee, that concludes my statement. I will be happy to take your questions.

[Prepared joint statement of Mr. Corbin and Ms. Garza follows:]

WRITTEN
TESTIMONY OF
KENNETH C. CORBIN
COMMISSIONER, WAGE AND INVESTMENT DIVISION
AND
SILVANA GINA GARZA
CHIEF INFORMATION OFFICER
INTERNAL REVENUE SERVICE
BEFORE THE
HOUSE OVERSIGHT AND GOVERNMENT REFORM COMMITTEE
ON THE FAFSA DATA RETRIEVAL TOOL
MAY 3, 2017

INTRODUCTION

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, thank you for the opportunity to discuss the work being done to secure the online Data Retrieval Tool (DRT) that is accessible from the fafsa.gov and StudentLoans.gov websites.

The IRS works continuously to safeguard our systems and protect taxpayer information. An important focus of this work is the ongoing battle against stolen identity refund fraud. We have made steady progress over the last few years in stopping fraudulent refund claims, criminally prosecuting those who engage in this crime, and helping minimize the adverse effect on taxpayers.

Despite all the progress we have made, the threat is constantly evolving. Fraudsters and criminal enterprises are using complex and highly sophisticated tactics to reach their target. As the IRS improves its capabilities and shuts off certain avenues of entry, identity thieves look for new ways of getting in. As the IRS enhances return processing filters and catches more fraudulent returns at the time of filing, criminals attempt to become more sophisticated at faking taxpayers' identities. We know we cannot rest and that solutions we implement are only good until the thieves find a new way to circumvent our defenses. We must stay diligent and ever watchful.

To address this challenge, the IRS is working not just to react better and faster, but to anticipate the criminals' next moves and stay ahead of them. To that end, we have used funding provided by Congress to increase our monitoring, detection, and analytical capabilities in relation to suspicious activity within our systems. These improvements have helped us slow down identity thieves, but we still need to do more. Congress helped us in this regard by approving $290 million in additional funding in 2016, which included $95 million to improve cybersecurity. We used a portion of that funding to implement the use of monitoring equipment and other capabilities that are more sophisticated than

what we had used previously. This has helped us detect suspicious activity in our various online tools and applications more quickly.

We have also undertaken a broad effort to review the authentication practices for programs where we share taxpayer information, and strengthen those practices where necessary.

One example of this effort was our decision last year to eliminate the electronic filing Personal Identification Number (e-file PIN) as an option for taxpayers to use to verify their identity when filing their tax return. Taxpayers received the e-file PIN by entering certain identifying information into an electronic tool on IRS.gov. After discovering unauthorized attempts had been made to obtain e-file PINs using data stolen from sources outside the IRS, we halted use of the e-file PIN. Although our analysis of the situation found that no personal taxpayer data was compromised or disclosed by IRS systems, we believe it was necessary to discontinue the e-file PIN to protect taxpayers and their data.

Our efforts to strengthen authentication practices also extend to programs where the IRS is authorized to share taxpayer data with organizations that use it to verify eligibility for customers who apply for loans. Since last summer, we have been working with banks, mortgage companies, and others to ensure they were implementing strong "know your customer" requirements.

Along those lines, in June 2016, the IRS announced new, stronger requirements for participants using the Income Verification Express Service (IVES). IVES is used by pre-screened companies who, in turn, are hired by mortgage firms and loan companies that need to verify applicants' income. Going forward, the IRS will only accept requests for taxpayer data from IVES participants who certify that they are using the new requirements to verify their clients. We took this step out of an abundance of caution to protect taxpayer information as well as safeguard IVES, which has been a successful program for the government, taxpayers, and the private sector since 2006.

THE FEDERAL STUDENT AID DATA RETRIEVAL TOOL

Applying for student financial aid is another area where we are concerned about the potential for bad actors to obtain taxpayer information fraudulently. We are working with the Department of Education to secure the online process through which student financial aid applicants obtain their federal tax information, which they need to complete the *Free Application for Federal Student Aid* (FAFSA®) or apply for an income-driven repayment (IDR) plan for their student loans. The focus of our concern is the Data Retrieval Tool (DRT), which allows an applicant to automatically populate the FAFSA, or an IDR plan application, with the required information from the applicant's tax return.

In the fall of 2016, we had an early indication of a potential misuse of the DRT to access taxpayer data. While the attempt was not successful, it highlighted the possibility that, with stolen personal information, a bad actor could pose as a student, begin completing an online application for student aid using the FAFSA, and give permission for the IRS to populate that application with tax data using the DRT.

Although the attempt failed, we immediately advised the Department of Education of our concern that criminals could access the tool and fraudulently obtain taxpayer data. We explored several potential solutions to address these concerns.

At the time, we agreed with the Department of Education that since we had no evidence of confirmed criminal activity and given that cutting off the tool could potentially increase the application burden for a large number of students and parents, we would not shut down the DRT immediately, but monitor usage, while we explored solutions that would meet both of our needs. We made this decision with the understanding that further action would be necessary if any indication of criminal activity was identified.

In early 2017, the IRS's Cybersecurity Fraud and Monitoring team observed anomalous behavior on the Federal Student Aid DRT using the IDR application. The IRS immediately increased monitoring and blocked Internet Protocol (IP) addresses based on the suspicious activity observed. The Department of Education performed additional analyses on the suspicious activity and determined that it was not fraudulent attempts to access tax data from the IRS.

Shortly thereafter, we learned of an incident that led us to determine that there was evidence of identity theft and likely fraud. Based on this incident, the IRS cybersecurity team was able to identify a pattern of suspicious activity. The pattern indicated criminals, having obtained personal information from sources outside the IRS, were masquerading as applicants for student financial aid and using the DRT to obtain enough tax return information to allow them to file fraudulent tax returns. The data obtained through the unauthorized use of the tool were later used, in some instances, in an attempt to file fraudulent returns. Having confirmed that the activity was fraudulent, we decided to turn off the DRT

STEPS TO HELP TAXPAYERS

The IRS is working to identify the number of taxpayers affected by questionable DRT use. We are also continuing to review the extent to which this contributed to fraudulent tax returns. We have identified some instances where our strengthened fraud reviews stopped a significant number of questionable tax returns by filers who accessed the DRT.

Our investigation of unauthorized attempts to access the DRT found that approximately 100,000 individuals may have had their taxpayer information compromised. We have mailed letters to these taxpayers to alert them to the possibility of suspicious activity related to their personal information, and to offer them free credit monitoring.

Along with notifying these taxpayers, the IRS is also marking their accounts to provide additional protection against the possibility that an identity thief could file a false return using their information. We are also giving these taxpayers the opportunity to obtain an Identity Protection Personal Identification Number (IP PIN). This will further safeguard their IRS accounts and help them avoid any problems filing returns in future years.

The roughly 100,000 taxpayers identified as potentially affected by this incident includes approximately 8,000 for which a return has been filed and a refund issued. We are analyzing these returns to determine if any of them are fraudulent.

IMPROVING E-AUTHENTICATION FOR THE DRT

The original IRS authentication process set up for DRT users to verify their identities was standard at the time the DRT was developed in 2009. This required users to provide their first and last name, Social Security Number (SSN), date of birth, tax return filing status, and address of record. .

We conducted an e-authentication risk assessment, completed last fall, which indicated the need for strengthened authentication procedures. Since then, we have worked collaboratively with the Department of Education to determine how best to strengthen these procedures, both for our DRT and their online FAFSA and IDR plan applications.

In working with the Department of Education, we recommended several potential solutions. We first looked at short-term solutions, but none of the ones proposed met all of the security requirements that we identified. The longer-term solutions we explored included the following:

- Strengthening user authentication protocols to a level to prevent unauthorized users from viewing tax return data using the DRT;
- Randomizing or obscuring the AGI and other data fields in such a way that what is viewed is not an exact depiction of the applicant data to be transmitted, making it less useful to criminals;
- Masking and encrypting the information so that the applicant would not be able to view it, but could still transmit it to the Department of Education;
- Exploring a legislative change to Internal Revenue Code section 6103 that would authorize the Department of Education to receive the data directly from the IRS, which would greatly increase security.

After consulting with the Department of Education we decided that, in the absence of legislation, the most effective solution would be to mask and encrypt the data, as envisioned in the encryption solution mentioned above, so that the data would not be visible to the applicant, thereby shielding information from last year's tax return from anyone masquerading as the student applicant. Randomizing or obscuring the information would not provide sufficient protection, and increasing the authentication procedure would make the tool unavailable to most applicants.

The option we chose balances the need to protect the taxpayer data while trying to make the solution accessible to the students applying for financial aid. The IRS is working toward an operational system upgrade for the IDR application by late May or early June 2017. The encryption upgrade is also planned the for 2018–19 FAFSA launch on October 1, 2017.

In the interim, families can still complete applications for student financial aid by manually providing the requested financial information from copies of their tax returns. And, if necessary, they can obtain a copy of those returns either online through the Get Transcript application, by mail, or from their tax preparer. Although we realize this is more burdensome than using the DRT, we have a responsibility to protect the DRT and all of our online tools from identity thieves. We will continue to discuss with the Department of Education other options for long-term solutions that ensure that the FAFSA remains accessible to everyone who wants to pursue postsecondary education while protecting sensitive taxpayer data.

Chairman Chaffetz, Ranking Member Cummings and Members of the Committee, that concludes our statement. We would be happy to take your questions.

Mr. RUSSELL. Thank you.

The chair now recognizes Mr. Camus for five minutes.

STATEMENT OF TIMOTHY P. CAMUS

Mr. CAMUS. Thank you. Chairman Russell, Ranking Member Cummings, and members of the committee, thank you for the opportunity to testify on the topic of the recent free application for Federal Student Aid data retrieval tool breach.

On average, each year the IRS issues approximately $400 billion in refunds, processes 242 million tax returns, and collects over $3 trillion in revenue. In addition to the significant amount of money that flows through the IRS each year, the taxpayers' IRS information is extremely valuable to identity thieves. As a result, the IRS has become a persistent target of cyber criminals located all over the world.

Over the past several years, TIGTA has conducted numerous investigations of a variety of cyber attacks on the IRS. For example, in May 2015 criminals launched a coordinated attack on the IRS e-authentication portal that was estimated to impact 110,000 taxpayers. Further investigation revealed that more than 700,000 taxpayers were impacted by abuses of the system by multiple bad actors over an extended period of time.

In January 2016, the IRS e-file PIN application was exploited. The IRS estimates the exploitation resulted in the issuance of over 100,000 e-file PINs that were used it to file fraudulent tax returns seeking more than $100 million in fraudulent refunds.

On January 25, 2017, the IRS noticed unusual activity on the FAFSA data retrieval tool. The IRS reported this observation to the Department of Education. The Department of Education advised the IRS that they believed the activity was legitimate activity.

Then, on February 27, 2017, it was determined that the FAFSA data retrieval tool was in fact being used in order to steal taxpayers' adjusted gross income, or AGI, information. Taxpayer AGI information is extremely valuable to identity thieves as it is needed by criminals in order to authenticate themselves for the purpose of filing fraudulent tax returns and stealing refunds.

Due to this activity, in early March 2017, the IRS made the decision to take the data retrieval tool offline. It is estimated at this time that as many as 100,000 taxpayers may have had their AGI information stolen through this exploitation.

Through the benefit of hindsight, all of these cyber-related incidents that I've discussed reveal that although the IRS conducts electronic risk assessments of its tax information sharing sites, it has had difficulty in identifying proper levels of risk associated with the various applications. That is because the struggle with determining the risk, then necessary authentication requirements, all the while balancing the ease of use for taxpayers, continues to be the challenge.

As we learn from our investigations how cyber criminals are defeating the various authentication and security requirements, we share what we learn with the IRS in order to help them shore up their applications. One thing is crystal clear. There is a determined criminal element paying close attention to electronic tax administration, and I believe these criminals will continue to present chal-

lenges to the future of efficient and secure electronic tax administration.

In summary, we at TIGTA take seriously our mandate to protect American taxpayers and the integrity of the IRS. As such, we plan to provide continuing investigative and audit coverage in the area of cybersecurity, and we look forward to continued discussions on ways we can fight these types of cyber crimes in the future.

Mr. Chairman, Ranking Member Cummings, and members of the committee, thank you for the opportunity to share our views, and I look forward to answering questions.

[Prepared statement of Mr. Camus follows:]

TESTIMONY
OF
TIMOTHY P. CAMUS
DEPUTY INSPECTOR GENERAL FOR INVESTIGATIONS
TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION
before the
OVERSIGHT AND GOVERNMENT REFORM COMMITTEE
U.S. HOUSE OF REPRESENTATIVES

"Reviewing the FAFSA Data Breach"

May 3, 2017

Chairman Chaffetz, Ranking Member Cummings, and Members of the committee, thank you for the opportunity to testify about the 2017 criminal exploitation of the Free Application for Federal Student Aid (FAFSA) and Data Retrieval Tool (DRT).

The Treasury Inspector General for Tax Administration (TIGTA) was created by Congress in 1998 to help maintain the integrity in America's tax system. It provides independent audit and investigative services to improve the economy, efficiency, and effectiveness of IRS operations. TIGTA's oversight activities are designed to identify high-risk systemic inefficiencies in IRS operations and to investigate exploited weaknesses in tax administration. TIGTA plays the key role of ensuring that the approximately 83,000 IRS employees[1] who collected more than $3.3 trillion in tax revenue, processed more than 244 million tax returns, and issued more than $400 billion in tax refunds during Fiscal Year (FY) 2016,[2] have done so in an effective and efficient manner while minimizing the risk of waste, fraud, and abuse.

TIGTA's Office of Investigations investigates allegations of IRS employee criminal and administrative misconduct, attempts to threaten or harm IRS employees, facilities or IRS data infrastructure, and external attempts to corrupt tax administration through the impersonation of IRS employees and programs, taxpayer data exploitation, and attempts to bribe IRS employees.

For the purposes of this hearing, my testimony will focus on the protection of taxpayer information, specifically the 2017 exploitation of the FAFSA application and the DRT.

---

[1] Total IRS staffing as of January 7, 2017. Included in the total are approximately 16,200 seasonal and part-time employees.
[2] IRS, *Management's Discussion & Analysis, Fiscal Year 2016.*

RECENT CHALLENGES IN SECURING TAXPAYER DATA

As cybersecurity threats against the Federal Government continue to grow, protecting the confidentiality of taxpayer information will continue to be a top concern for the IRS and for TIGTA. According to the Department of Homeland Security's U.S. Computer Emergency Readiness Team, Federal agencies reported 77,183 cyberattacks in FY 2015, an increase of approximately 10 percent from FY 2014. The increasing number of data breaches in the private and public sectors means more personally identifying information than ever before is available to unscrupulous individuals.

Due to the $400 billion dollars the IRS issues in refunds and the 242 million tax returns it processes each year that contain extremely valuable information for identity thieves, the IRS has become a favorite target of cyber criminals located all over the world. For example, in May 2015, criminals launched a coordinated attack on the IRS e-Authentication portal that resulted in the exploitation of the IRS Get Transcript Application, as well as the IRS IP PIN application. It is estimated that more than 110,000 taxpayers were impacted by this attack.

A subsequent review of all of the activity on the system revealed that more than 700,000 taxpayers were impacted by similar abuses of the system by multiple bad actors over an extended period of time. In January 2016, a coordinated effort was launched that exploited the IRS Electronic Filing PIN (e-File PIN) tool. The e-File PIN tool was created to provide taxpayers with a special PIN number that would allow the taxpayer to electronically file a Federal tax return. The IRS estimates the exploitation resulted in the issuance of over 100,000 e-File PINs that were used to file over $100 million dollars of fraudulent tax returns. As a result of this exploitation, on June 23, 2016, the IRS announced that it had disabled the e-File PIN application. Numerous investigations are underway on the individuals who obtained taxpayer information from both of these attacks.

FAFSA AND THE DRT

The DRT allows students and parents to access their adjusted gross income (AGI) information through an interface with the IRS to complete the FAFSA by transferring the AGI information directly into their FAFSA application form. FAFSA on the web was first introduced in on June 30, 1997 and the IRS DRT component of the process was activated on January 28, 2010.

Following the e-Authentication Get Transcript exploitation in May 2015, the IRS reevaluated the authentication risk on outward-facing online applications based on today's known cyber-crime environment. The IRS conducted this e-Authentication Risk Assessment (eRA) on 45 applications, including the FAFSA and DRT process. On October 25, 2016, the IRS determined the risk factors involving financial loss or agency liability, harm to agency programs or public interests, and the risk of unauthorized release of sensitive information utilizing the FAFSA and the DRT were all scored in the low risk category. On December 5, 2016, the Risk Assessment Form and Tool was signed by the IRS, and the FAFSA and DRT remained operational.

It appears that identity thieves used personal information of individuals that they obtained outside the tax system to start the FAFSA application process in order to secure the AGI tax information through the DRT. The IRS' current estimate for the number of impacted taxpayers is approximately 100,000. TIGTA is conducting a joint investigation of this exploitation with IRS Criminal Investigation and the Department of Education Office Inspector General (Education OIG). As part of our investigation, we are also looking back to see if there was an earlier bulk exploitation of the FAFSA and the DRT process. TIGTA is also planning to initiate an audit to review this issue.

In September 2016, TIGTA detected an attempted access to the AGI of a prominent individual. When we investigated the attempted access, we determined that the FAFSA application and the DRT were used in this attempt. Since FAFSA is a Department of Education application, we notified the Education OIG and we notified the IRS Privacy, Governmental Liaison and Disclosure (PGLD) program office. We initiated a joint investigation with the Education OIG that included the Cyber Crimes Task Force. The investigation identified the individual responsible for the attempted access and he was arrested. This case is still proceeding through the court system. In November 2016, we noticed another attempted access of the same prominent individual's AGI through the FAFSA and the DRT, this time, from an entirely different location. We have included this attempted access in our investigation activity and we also notified the PGLD program office. This activity is still under investigation.

On January 25, 2017, the IRS reported to us that a high number of Taxpayer Identification Numbers were being processed through FAFSA and the DRT. The IRS told us that when they shared this observation with the Department of Education, Education told the IRS that they believed the activity was related to student loan consolidation activity.

On February 27, 2017, a complainant reported that he received a copy of his tax transcripts at his home with a letter telling him that he had requested them. The complainant reported he never ordered a copy of his tax transcripts. When his tax account information was researched, we learned that the complainant's AGI had been accessed through the FAFSA and the DRT process. As a result, we determined that the January activity that the IRS observed was proof that an exploitation was under way. Initial analysis showed there were 8,000 questionable accesses at that time.

On March 3, 2017, the IRS reported that they disabled the DRT due to privacy concerns and to protect sensitive taxpayer data.

We are continuing our criminal investigations of this activity and are reviewing evidence and information obtained from the investigations of the prior e-Authentication exploitations to determine if the FAFSA and DRT criminal activity was launched by the same individuals and groups. In one instance, we found evidence that as far back as February 2016, the subject of an e-Authentication investigation discussed the availability of AGI information using FAFSA and the DRT. After comparing additional log file information and email addresses, we now have very good indications that in some instances, the same individuals and groups engaged in criminal activity on the e-Authentication portal are involved in this exploitation of the FAFSA and the DRT.

We at TIGTA take seriously our mandate to provide investigative coverage of issues that confront the IRS in its administration of our Nation's tax system. As such, as we conduct our investigations of the criminals who are responsible for the cyber exploitations, we share the information we find with the IRS in order to help protect the IRS' data infrastructure. We plan to provide continuing coverage of the IRS' efforts to operate free from criminal activity in the electronic environment.

Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee, thank you for the opportunity to share my views.

Mr. RUSSELL. Thank you.

The chair will now recognize himself or five minutes.

Ms. Garza, you know, as I look at this situation—and you certainly have a lot of experience both in the CIO arena, as well as in public service, and we do appreciate that. A lot of times public servants are taken for granted. But with your broad experience, that is not taken lightly. But still, as we examine this issue, we are trying to get to who is responsible for making the operational and security decisions for the data retrieval tool?

Ms. GARZA. Sir, as I said in my opening testimony, we are all responsible for ensuring that cybersecurity is our top priority. As a group, we look at every risk assessment, we evaluate the situation, and we make the decisions as to what level of risk we're willing to take with the application that we are talking about.

Over the last year since Get Transcript, we've become much more conservative, but we evaluate the situation, we discuss it, and we determine what actions we need to take.

Mr. RUSSELL. Now, in your testimony you had mentioned that this was unique because, unlike attempts or attacks on the IRS and the different departments within the IRS, this involved a different department. So you had one end of the pipe and the other end of the pipe. So when you learned in September 2016 that it was possible to, with, quote, "little stolen personal information," for a hacker to pose as a student and access the DRT tool and the data stored on that tool, why did you not move to immediately secure the tool through encrypting or otherwise masking the sensitive information accessible through the DRT?

Ms. GARZA. So there was a couple of actions that we took at that time. We—first of all, there was no data loss at the time. We had no evidence of fraud at the time. We immediately ——

Mr. RUSSELL. Well, there was no evidence of fraud but that doesn't mean that there wasn't. I mean, you had a clear indication that something was awry, yes or no?

Ms. GARZA. We looked at the analytics and we looked at all of the data that we had available to us at the time, and we did not see anything suspicious. We contacted the Department of Education. Our—both cyber organizations started to work to look at the data, and the data did not reveal that there was any kind of penetration going on at that time.

Mr. RUSSELL. Well, didn't—and I guess—you know, and here is the information I am speaking at specifically. You know, the isolated case, did it not result in an indictment that is still processing in the courts from September 13?

Ms. GARZA. It was a single case, and they did not get the data.

Mr. RUSSELL. Well, I guess then let me follow on this vein because what I hear each of the panelists saying is that no data breach, no problem, and I hear Mr. Camus say 100,000, investigation ongoing, and fraudulent returns filed, and I will come back to some of that. But, Mr. Gray, to what extent do you think that the Department is responsible for securing the data accessible on FAFSA.gov and other web-based applications?

Mr. GRAY. One hundred percent we're responsible for securing our data.

Mr. RUSSELL. Okay. But yet we see what the Department of Ed saying, hey, give us the tool, we have the IRS saying here is your tool and you have got data coming out the spigot on one end, you think it is secure on the other, there is a leak, and yet it took you how many months from September to February to even recognize and say, no, we thought it was legitimate in September but now we think we might have a problem. That is a big period of breach. So would you say that you have a responsibility for—you do have that responsibility, but that wasn't perceived as such in September?

Mr. GRAY. It was perceived that there was a potential vulnerability in September, October, and the two departments worked together to create a solution that would prevent that vulnerability from being exploited. It did—when it became an exploited vulnerability, which was in March, is when we took the appropriate action to bring it offline.

Mr. RUSSELL. And yet it wasn't shut down when you had indication in the start of a new financial aid season. And I guess what I would like to do is—you know, Mr. Runcie, you said that there was no evidence that info was accessed, but were fraudulent returns filed with regard to this data?

Mr. RUNCIE. Mr. Chairman, I can't tell you if fraudulent returns were filed or not. What I can tell you— because we're not privy to that information. What we did was we analyzed the Social Security numbers, IP addresses. We did a pretty exhaustive examination looking at indicators of risk, and we returned that information to the IRS so that they could complete some of their analysis.

In September, as I mentioned earlier in my oral comments, we at that point probably had filed 50 million applications using the DRT. So we filed a substantial amount of applications using the DRT going back seven years to 2010.

It is an evolving landscape and it's quite possible, as we've said, that the criminals and the fraudulent activity, you know, they're innovative and so things change. But over that period of time there wasn't any documented material criminal activity on the DRT. When that was found and confirmed, it was shut down. So there's a history there that—one we relied on even though we continued to monitor it, and we balanced that against the risk of shutting off the tool and all the implications around shutting off the tool.

Mr. RUSSELL. Well, there is always a risk of protecting taxpayers, and I want to be respectful of the time here. But before I turn it over to the ranking member, you know, what it appears is that we are not identifying that we had a breach and it has made us more vulnerable. And with that, we will come back to some of that at a later time.

I would like to recognize the ranking member, Mr. Cummings.

Mr. CUMMINGS. Thank you very much, Mr. Chairman.

Mr. Runcie, this past September, the inspector general issued a scathing report warning that student loan companies were using the Federal aid website to take advantage of students. The IG explained the tactics these companies were using to commit possible fraud. First, the loan companies would obtain the logon credentials students used to access their accounts. Then, the loan companies would change or create new credentials to let them take control of

the student accounts. These loan companies took advantage of the students for commercial gain in many different ways. Now, Mr. Runcie, are you aware of that report?

Mr. RUNCIE. Yes, I am.

Mr. CUMMINGS. And in one case the IG reported that a loan consolidation company, and I quote, "changed the mailing address, phone number, and email address for borrowers so that it would be difficult for borrowers to be contacted by their own loan servicers." Another company charged students $60 monthly service fee to, and I quote, "put their loans into forbearance with the stated promise of eventually enrolling them in the Public Service Loan Forgiveness or some other debt reduction program even though the borrowers in some cases were not qualified for these programs."

Now, Mr. Runcie, when you read this report, were you troubled by these companies that did this to these students?

Mr. RUNCIE. Ranking Member Cummings, yes. I think we were all troubled. And we continue to work with the IG. We have a potential solution or mitigating action that we're going to take later this month. So we understand what the issue is. But as you mentioned earlier, there is the technicality of someone who potentially signs up for these services. So whether it's through power of attorney or some other agreement, there is sort of that technical issue that we have to deal with.

Mr. CUMMINGS. So the IG reported that it could not prosecute these loan companies based on technicalities. For example, many of these companies required students to sign those powers of attorney in order to get the loans. The companies that used these powers of attorney to improperly access the student accounts. Now, Mr. Runcie, it should not be necessary for students to sign powers of attorney to get student loans. Do you agree with that?

Mr. RUNCIE. Yes, I absolutely agree. And I think one of the approaches that we've taken is to go heavy on user education. I mean, ultimately, all these services that are being provided can be done free. But again, through aggressive marketing tactics and so forth, it's quite possible that there are number of people who are not aware that they can get these services done free. So we've been real focused on user education, and in addition, you know, we're going to make sure that there's information out there that the IG can leverage in terms of going after some of the bad actors that are out there, and that's what I referenced a little bit earlier without actually being specific.

Mr. CUMMINGS. I got you. Now, what other actions have been taken so that going forward these student loan companies will be held accountable for these abusive activities? I just think there is something about this that just tears at my heart because I see so many—a sit on the board of a college, and I see young people having to drop out of school because they don't have money and they are struggling. They just want to go out there and be all that God meant for them to be. And not only do they have to fight people who are supposed to be helping them, but then they lose the opportunity. And they don't lose it maybe for a week or a day. They lose it for a lifetime. That is why I am so concerned about this.

Now, what assistance can Congress provide to help hold student loan companies more accountable? What can we do? Do you need some help?

Mr. RUNCIE. Yes. I mean, you know—while I have some thoughts ——

Mr. CUMMINGS. Give us your thoughts because we have a duty. Once we find out that there are things that we can do, we need to explore to try to figure out whether they are practical to be done ——

Mr. RUNCIE. Yes, well ——

Mr. CUMMINGS.—but we have got to know what they are.

Mr. RUNCIE. Yes. I mean, so there is that technicality. I don't know if there is a way to sort of limit the ability to transfer the authority of giving away your password and your information so that others can provide those services. If there is some, you know, legislative process to address that, then, you know, I would be an advocate of it.

I think the other thing, though, is you've got a balance that potentially with there may be a population—and I know it's—it would be a segment, a small segment of the people that are being contacted who may actually need some guidance for some—whether it's loan consolidation or providing some other, you know, value within the Federal Student Aid system. There may be some small amount, and we would have to sort of think about the impact on those that might need some level of assistance.

But again, I think the bigger problem is what you indicated. There is the potential for people to be put in a situation where they're harmed for a very long period of time because they're not educated about some of the options out there to do it by themselves.

Mr. CUMMINGS. So would you think legislation regarding the—doing away with the power of attorney requirement would be appropriate?

Mr. RUNCIE. I think it would be something that we should consider. You know, again, I—we'd have to do some analysis, you know, and it could be surveys or whatever. There are—like I said, there's potentially a group of some of the most needy who may need some assistance, and I can't calibrate that right now. But I think, as you said, the bigger problem is that there's a lot of them that aren't aware that they don't need to pay for these services and are being exploited.

Mr. CUMMINGS. Mr. Chairman, I would hope that we would pursue this even further. I think it would be legislative malpractice for us not to protect these students. It is ridiculous that we—we have got a do all that we can. I am sure that you will work with us and everybody up there on our panel work with us try to make sure that happens.

The other thing that we have got to do, Mr. Chairman, we can't have just a hearing with these folks. We have got to bring in these people that are messing over our young people and playing games with their lives. And so I look forward to working with you and Chairman Chaffetz as we move forward.

Mr. RUSSELL. And I thank the ranking member and agree that, you know, it extends even beyond the students. It extends really

to all Americans. This is very private data and even to their parents and others and look forward to working that effort.

The chair would like to recognize now the gentleman from North Carolina, Mr. Walker, for five minutes.

Mr. WALKER. Thank you, Mr. Chairman.

Mr. Camus, I want to ask you to describe the following three incidences, but I would just like for you to confirm them if you would, please, specifically the ones starting in September 2016. Was that incident involving the data retrieval tool, was that criminal in nature?

Mr. CAMUS. Yes, it was.

Mr. WALKER. Okay. Did the incident result in an indictment?

Mr. CAMUS. Yes, it did.

Mr. WALKER. Okay. There was also one that was identified in November 2016 and the third one was on January 25, 2016, by which a high number of taxpayer identification numbers were identified as being processed on the FAFSA that raised red flag. Did this result in a notification of a major incident to Congress?

Mr. CAMUS. No, it did not.

Mr. WALKER. Okay. Ms. Garza, given the three separate incidents as described by TIGTA that predated the major incident that resulted in the DR tool not being taken offline on March 3, the question is why was the data retrieval tool not taken offline earlier?

Ms. GARZA. So ——

Mr. WALKER. Microphone, please. And if you would, just could you pull that microphone a little closer and speak into it there? Thank you.

Ms. GARZA. Thank you, sir. Congressman, in regard to the September incident, we took immediate action by analyzing the data that we have, and we found that there was no evidence of a breach. The data was not lost. And we started working with the Department of Education to strengthen the authentication process for the data retrieval tool.

I am not aware of the incident in November and so I will have to go back and look at what the findings were for that.

Mr. WALKER. Yes. I don't understand the fact as far as saying, well it wasn't breached, it wasn't breached. I was just listening thinking of my family back home. If I have got a security system, yet we have still people trying to break into that, at some point I am going to be concerned, say, well, oh, nothing was taken, nobody was hurt, nothing was damaged. It doesn't make sense to me that there is not more action being taken here. Shouldn't the IRS be concerned about criminal misuse of the tool being sufficiently perked? Is that not something that is important?

Ms. GARZA. Protecting the taxpayer data is our top priority. We had to—we're trying to balance the protection of the taxpayer data with the use of the tool, and that is why we reached out to the Department of Education to have discussions about what we could take. We saw this is action that we needed to take immediately, and we did take that—those actions to come up with—to try to come up with a solution that would mitigate the risk.

Mr. WALKER. Now, the keyword is trying to come up with a solution. I am not sure we have arrived at that. And according to Mr.

Runcie's written testimony, after the October 2016 discovery that the DRT could potentially be vulnerable, the IRS increased monitoring of the tool for any suspicious activity. Could you describe what that increased monitoring looked like?

Ms. GARZA. That is correct. We—actually, we engaged with our TIGTA friends and asked them, as well as the new cyber analytics team that we have in place, to start looking for suspicious activity. And actually it was because of that increased monitoring that we had done that we identified that there was suspicious activity occurring in January.

Mr. WALKER. Yes. There was an incident also in February of this year, I believe. Was that discovered by accident?

Ms. GARZA. We have mechanisms in place, multilayer defense mechanisms. One of the mechanisms is a notification to the address of record to the individual whose data has been identified. That actually led us to identify that we had an issue. As we investigated that issue, we were able to find that in fact there was a fraud that had taken place and we immediately shut down the application.

Mr. WALKER. So for the record you are saying that no, that it wasn't discovered by accident?

Ms. GARZA. There was a notice that was generated to the taxpayer that had that taxpayer come in and notify us that there was something amiss.

Mr. WALKER. To me this is not only a question of taking responsibility for the IRS and Department's web-accessible services and data but of understanding the cybersecurity risks these online services and applications face. And I certainly agree with the Ranking Member Cummings. These are young people's lives at stake, and to—as they are coming out and getting started, to be able to put them on a path where they are having to unravel this, I hope there is more of a sense of urgency to deal with this issue than what presently seems to be at the time.

With that, Mr. Chairman, I yield back.

Mr. RUSSELL. The gentleman yields back.

And the chair would now like to recognize the gentlelady from New Jersey, Mrs. Watson Coleman, for five minutes.

Mrs. WATSON COLEMAN. Thank you very much, Mr. Chairman, and good morning to all of you.

Mr. Runcie, in September the inspector general reported that student loan companies misused the Department's system to take advantage of students. As reprehensible as this finding is, this is not the first time student loan companies have acted against the best interests of the students they are supposed to be serving. In 2015, the Consumer Financial Protection Bureau and the Department conducted a public inquiry finding a vast universe of complaints regarding loan servicers.

And even more concerning, this current administration has withdrawn a series of policy memos that have been issued from the previous administration that were put in place to strengthen protections for student loan borrowers. Mr. Runcie, what impact would this action have on student loan borrowers? And do you think that this could aggravate the issue of predatory lending practices?

Mr. RUNCIE. Well, in terms of our focus, you know, our focus from a servicing perspective is to make sure that we have the highest quality outcomes for all the students and borrowers. And, you know, we've done a—we've put in place a series of actions over the years, and right now, we're going through a re-competition among the servicers that you referenced. Because we're in a procurement process, I can't really talk about specifics, but I will just reiterate that we are focused on having the highest quality product that we can from a servicing perspective and generating the best outcomes for students and borrowers.

Mrs. WATSON COLEMAN. Are you aware of the rollback of certain oversight and accountabilities that had been instigated or initiated in this administration that are overturning some of those accountabilities that were designed to protect students and vulnerabilities?

Mr. RUNCIE. I personally am not aware of any rollbacks.

Mrs. WATSON COLEMAN. Is there anyone on this panel that has any knowledge of any recent actions on the part of either this administration through the White House or the Department of Education that will negatively impact the accountability of who is and who is not a good person or entity to work in this space? Is that a no? There is no one?

Ms. GARZA. No.

Mr. GRAY. No.

Mr. CORBIN. No.

Mrs. WATSON COLEMAN. Interesting. Okay. This January, the Consumer Financial Protection Bureau filed a lawsuit against one of the Nation's largest servicers of Federal and private student loan Navient. According to the lawsuit, Navient cost borrowers billions of dollars by withholding information about income-based repayment programs that could have lowered borrowers' monthly payments. Instead, they reportedly pushed borrowers into forbearance, suspending their payments but not the accrual of the compounding interest. Mr. Runcie, are you familiar with these allegations in CFPB's lawsuit?

Mr. RUNCIE. Yes, I'm familiar with those allegations.

Mrs. WATSON COLEMAN. Navient services the student loans of more than 12 million borrowers and roughly 6 million of whom are serviced to contractors with the Department of Ed. Is that so?

Mr. RUNCIE. I believe that's right.

Mrs. WATSON COLEMAN. And Navient sought to dismiss CFPB's complaint as part of its defense. It alleged, and I quote, "the servicer acts in the lender's interest and there is no expectation that the servicer will act in the interest of the consumer." Is that right?

Mr. RUNCIE. I'm sorry. I didn't hear the last part.

Mrs. WATSON COLEMAN. The servicers—the servicer ——

Mr. RUNCIE. Yes.

Mrs. WATSON COLEMAN.—acts in the lender's interest and there is no expectation that the servicer will act in the interest of the consumer.

Mr. RUNCIE. Yes, I understand that statement. In the case of, you know, private lenders, a servicer would be acting on the behalf of private lenders. That's right.

Mrs. WATSON COLEMAN. Does it concern you that companies like Navient publicly claim they have no responsibility to act in the best interest of the students they are supposed to be serving?

Mr. RUNCIE. We are currently in a procurement process and I can't make a comment on that, of which Navient is also in the procurement process so I can't make a comment on that. We're making decisions about our servicers.

Mrs. WATSON COLEMAN. All right then. I would expect that what you were going to do is to look at information such as this and not—we are not going to ask you again about someone like Navient even though you can't express whatever is happening with regard to the company right now.

Mr. RUNCIE. You know, what I can say is, I mean, we look at past performance, we look at responsibility metrics. There are criteria that we have to look at in terms of the process but ——

Mrs. WATSON COLEMAN. Well, I don't know by number the executive order or the rollback that just took place as it relates to looking back at a company's business and reputation, but I think that is something you need to look at to see whether or not it does negatively impact your ability to ensure that the best is taking care of the best.

Mr. RUNCIE. Absolutely.

Mrs. WATSON COLEMAN. Thank you. And with that, I yield back.

Ms. FOXX. [Presiding] The gentlewoman yields back.

The gentleman from Ohio, Mr. Jordan, is recognized for five minutes.

Mr. JORDAN. I thank the chair.

Mr. Corbin, when did the IRS notify TIGTA that you guys had a problem?

Mr. CORBIN. Sir, the notification to TIGTA for the incident on February 27 happened that same day.

Mr. JORDAN. So you guys talked to Mr. Camus and his guys on February 27 of this year?

Mr. CORBIN. I did not personally talk to Mr. Camus ——

Mr. JORDAN. Someone at the IRS?

Mr. CORBIN.—but someone at the IRS did, yes, sir.

Mr. JORDAN. Got it. And how many taxpayers are potentially harmed by the hacking and the breach that took place?

Mr. CORBIN. Approximately 100,000, sir.

Mr. JORDAN. Hundred thousand people. And then the law requires you to notify Congress when something like this happens, doesn't it?

Mr. CORBIN. I'm not familiar with that, sir.

Mr. JORDAN. Well, I will read it to you. This is a letter from your boss, Mr. Koskinen. The Federal Information Security Modernization Act and criteria provided in the Office of Management and Budget guidance says this, that not later than seven days after the date of an incident you should notify Congress, right?

Mr. CORBIN. Correct. Yes, sir.

Mr. JORDAN. Okay. So you are supposed to do it and you are supposed to do it within seven days. Is that accurate?

Mr. CORBIN. That sounds accurate, yes, sir.

Mr. JORDAN. Okay. It doesn't just sound accurate. That is the law.

Mr. CORBIN. Yes, sir.

Mr. JORDAN. So when did you tell Congress?

Mr. CORBIN. Sir, I believe we notified Congress within that seven-day timeframe from what I know.

Mr. JORDAN. Really. Is that true, Mr. Camus?

Mr. CAMUS. Mr. Jordan, I'm not sure when they made notification to Congress.

Mr. JORDAN. Because we don't have it until April 6, which is a lot longer than seven days. You learn on February 27, you tell Congress on April 6.

Mr. Corbin?

Mr. CORBIN. I'd have to go back and check that, Congressman.

Mr. JORDAN. Well, that is important, right?

Mr. CORBIN. Yes, sir.

Mr. JORDAN. Mr. Koskinen testified on April 6 and that is when he told us.

Mr. CORBIN. Well, I ——

Mr. JORDAN. He testified in front of the Senate.

Mr. CORBIN. Yes, Congressman. I'd have to go back and take that back and confirm that for you, sir.

Mr. JORDAN. Well, I don't know that—well, we would appreciate that, but this is when Congress first learned was on April 6 that there had been an incident. And here is what the statute says. It says, "not later than seven days after the date on which there is a reasonable basis to conclude that a major incident has occurred." Would you describe this as major, Mr. Camus?

Mr. CAMUS. The fact that it impacted potentially 100,000 people, I would say so.

Mr. JORDAN. Same here. So we are wondering why you waited so long.

Mr. CORBIN. I don't have an answer to that, Congressman. I'll go back and find out for you.

Mr. JORDAN. Well, we would like to get that because, frankly—well, let me turn to Mr. Camus.

Mr. Camus, is this the first time the IRS has waited to tell Congress some important information?

Mr. CAMUS. Mr. Jordan, I'm not aware. I can't answer your question.

Mr. JORDAN. Well, maybe I will refresh your memory. There was a little incident that happened over the last several years where the Internal Revenue Service systematically and for a sustained period of time targeted taxpayers based on their political beliefs. Are you familiar with that situation, Mr. Camus?

Mr. CAMUS. I am familiar with that.

Mr. JORDAN. You did an investigation into that, didn't you?

Mr. CAMUS. Yes, sir.

Mr. JORDAN. A couple of investigations ——

Mr. CAMUS. A couple.

Mr. JORDAN.—didn't you?

Mr. CAMUS. Yes, sir.

Mr. JORDAN. Yes. And was the IRS always forthcoming in a timely fashion with important information in that investigation you did, Mr. Camus?

Mr. CAMUS. We found that there were some mistakes that were made and some materials that should have been turned over, that's correct.

Mr. JORDAN. Well, that is a nice way of saying it. I appreciate that. You have got maybe a career in politics after you are done at TIGTA, Mr. Camus, with that answer.

Let me just refresh your memory. The IRS knew there was a gap in Lois Lerner's emails in February 2014. They did nothing to stop the destruction of backup tapes, actually 421 backups. You remember this, Mr. Camus?

Mr. CAMUS. Yes, sir, I do.

Mr. JORDAN. Because it was your investigation that discovered they destroyed 421 backup tapes, right?

Mr. CAMUS. That is correct, sir.

Mr. JORDAN. Potentially 24,000 emails, right?

Mr. CAMUS. Yes, sir.

Mr. JORDAN. And that all happened in March 2014, a month after they knew there was a gap in her emails. And Mr. Koskinen testified in April of 2014, but what you know what he told Congress? June 13, 2014, is that right, Mr. Camus?

Mr. CAMUS. That's correct.

Mr. JORDAN. So here we have again the Internal Revenue Service, an agency that has a little bit of influence and impact on American people's lives, with a major breach that the law says you are supposed to tell Congress within one week, within seven days. And what did they do? They wait 38 days. And you know what—to add insult to injury, think about what Congressman Walker just talked about, all the suspicious activity that took place before February 27.

In fact, when Mr. Koskinen testified and said, oh, we are putting you on notice, Congress, that there has been a major breach, 100,000 taxpayers potentially impacted, look at what he said in that testimony. He said this: April 6, 2017, Mr. Koskinen testified in front of the Senate Finance and said, quote, "We have started working with Education in October telling them we were very concerned,"—very concerned—"that the system could be utilized by criminals."

So Mr. Koskinen was on notice that there was problems, potential problems, potential big problems. He even used the term "very concerned" clear back in October of last year. We have the major breach take place on the 27th when the IRS tells you, hey, guys, we have got to look into this; this is real. We have had all these things happen, suspicious activities ahead of time, and they don't comply with the law and tell Congress within a week. They wait 38 days to tell us. It is not supposed to be how it works, is it, Mr. Camus?

Mr. CAMUS. It doesn't sound so, sir.

Mr. JORDAN. No. And the IRS—once again, the IRS is treating taxpayers the way they are not supposed to, and it is why this committee has been so focused on trying to clean up the mess over there and frankly I have been so focused on saying Mr. Koskinen has to go.

With that, I yield back, Madam Chair.

Ms. FOXX. Thank you, Mr. Jordan.

Ms. Plaskett, you are recognized for five minutes.

Ms. PLASKETT. I want to thank the lovely chairwoman this morning for the opportunity to speak.

Thank you all for being here. Of course, everyone on both sides of the aisle are very concerned about this issue. Most of us have children and have our own student loans or have loans that we are helping with the children that we care very much about our future, as well as our constituents'.

I did, however, just want to touch on something that I know one of my colleagues spoke about just a few moments ago, Mr. Runcie, when they talked about the lawsuit with Navient. It is, however, understood that this is a lawsuit so the interest of both parties—you know, they both have allegations raised. But Navient does have a lower default rate than some of the other users or loan companies that—and they do have a propensity to loan to minority and underserved communities, is that correct? I understood that the default rate of the students who have loans with Navient is a significantly lower potentially than some of the other loan companies.

Mr. RUNCIE. I would have to confirm that. And a lower default rate is better, right?

Ms. PLASKETT. Right.

Mr. RUNCIE. Yes.

Ms. PLASKETT. Yes.

Mr. RUNCIE. But I'd have to confirm that.

Ms. PLASKETT. Okay.

Mr. RUNCIE. And I know the portfolios aren't all the same. They have different compositions and so sometimes there would be natural, you know, differences in the default rates for the various services.

Ms. PLASKETT. Sure. Sure. Okay. So one thing that is really interesting as well, Mr. Runcie, when we are talking about the inspector general's report, it seems, you know, something that we are all very focused on. And the IG warned that the systems were, and I quote, "being misused by commercial third parties to take over borrower accounts." This is something that Ranking Member Cummings talked about. These are things that we are really very keen on because these are of course students who are navigating a very difficult system. This is sometimes some of the first instances where they are really delving into their own finances, making decisions that are going to have an impact on them for the rest of their lives.

So the commercial third parties are student loan companies and student loan consolidators. Is that correct when we are talking about ——

Mr. RUNCIE. That is right.

Ms. PLASKETT.—the third parties that take over borrower's accounts? And less than two weeks ago this committee conducted an interview with the special agent in charge of conducting that investigation for the IG, and he explained to the committee that the information in these students' accounts is, quote, "of commercial interest for loan consolidators." Right?

Mr. RUNCIE. Yes.

Ms. PLASKETT. And that word commercial interest is very key to me. He also told us that student loan companies, and I quote,

"were controlling thousands of accounts or creating thousands of accounts and controlling them." Mr. Runcie, is this true? Were student loan companies actually using the information of individuals they are there to serve in a manner to control for commercial interests those accounts?

Mr. RUNCIE. Yes. My understanding is that they—it's a fee-for-service, and so to the extent that they've got 1,000 clients, they're being charged for those services. So it would be a commercial endeavor.

Ms. PLASKETT. And do you have a list of the names of those companies that were doing that?

Mr. RUNCIE. We've identified some. I don't know that we have an exhaustive list of those companies.

Ms. PLASKETT. Ms. Chairwoman, may I ask that we obtain a list of every student loan company that were involved in the activities?

And, Mr. Runcie, how long would it take you to provide something like that to the committee?

Mr. RUNCIE. I don't want to commit because I'm not sure how readily available ——

Ms. PLASKETT. Come on, you can't give me like, you know, an outside range time or anything like that? A week, two weeks, a month?

Mr. RUNCIE. I'd say if you'd give us a month, that would be appreciated.

Ms. PLASKETT. Of course you would for the outside of what I requested.

Mr. RUNCIE. Hey, I don't want to negotiate against myself.

Ms. PLASKETT. Got you. Got you. Got you. Very good.

Ms. PLASKETT. The special agent in charge also told us that student loan companies were, I quote, "aggressively pursuing account holders and taking advantage of this." That sounds outrageous. And could you explain to me not just with the aggressively pursuing but what did he mean by taking advantage of them?

Mr. RUNCIE. I don't want to speculate, but, you know, to the extent that they're providing services and they have account information, you know, they can receive correspondence on their behalf and make decisions on their behalf. And those decisions might benefit them commercially.

Ms. PLASKETT. And are any of these same companies still doing business with the Department of Education?

Mr. RUNCIE. Not that I know of.

Ms. PLASKETT. Okay. Ms. Chairwoman, we have a responsibility to help protect students from the kind of abuse, and I am so very pleased that we are having this hearing to go through this. And I believe the entire committee is very keen on holding a follow-up hearing within the next—with the student loan companies that are actually engaged in these activities. And I hope that we can have the IG from the Department of Education testify about what they have found.

Thank you very much for the information that you have provided us, and I hope, Ms. Chairwoman, we are able to do that. I yield back.

Ms. FOXX. Thank you, Ms. Plaskett. First of all, I want to say thank you for your willingness to accommodate me on the Floor the other night. It wasn't necessary, but I appreciate that.

And I believe under the committee rules you have the right to ask any witness for any information, and I am sure that will be followed up with the staff. So thank you very much.

Mr. Hurd, you are recognized for five minutes.

Mr. HURD. Thank you, Madam Chairwoman.

I apologize if I review some information that has already been discussed in this hearing. But raise your hand— and this is for all five of you—raise your hand if you are responsible for FAFSA.gov.

All right. Let the record reflect Mr. Runcie, Mr. Gray, and Ms. Garza raised their hand.

Raise your hand if you are responsible for the DRT tool or also known as the FSA–D tool?

All right. Let the record reflect Ms. Garza and Mr. Corbin raised their hand.

In October 25, 2016 IRS, conducted an e-authentication risk assessment, and it concluded that the DRT tool was in need of stronger authentication measures. Is that correct, Ms. Garza?

Ms. GARZA. Yes, it is, sir.

Mr. HURD. And were steps taken to improve the authentication measures?

Ms. GARZA. We started to work with the Department of Ed ——

Mr. HURD. You started to work with the Department of Ed. What steps—what did you actually do since October 25, 2016 to strengthen the DRT tool?

Ms. GARZA. We increase monitoring on that application so that we could become alerted should something—we see something suspicious.

Mr. HURD. Were those efforts successful?

Ms. GARZA. In January it was those efforts that identified that there was a suspicious activity occurring, and at that time we partnered with the Department of Ed to get our two cyber teams together to review that suspicious activity. And we were informed by the Department of Ed that that was not—it was normal behavior.

Mr. HURD. What steps are being taken now to strengthen the authentication of DRT?

Ms. GARZA. We have already developed and implemented an encryption solution on the IRS side. We are working with the Department of Ed ——

Mr. HURD. How is encryption going to help with authentication if you have a user that has stolen credentials?

Ms. GARZA. The authentication solution that we had looked at was not satisfactory to provide the usability of the application, so we have moved to an encryption. So unless that ——

Mr. HURD. But that doesn't answer the question. The question is how does encryption on the backend help with authentication of an attacker that is using stolen credentials?

Ms. GARZA. It does not improve authentication. What it does do is does not allow the data to be revealed to someone other than the actual applicant.

Mr. HURD. But if you have stolen credentials and you are able to spoof that, you have the credentials, what are you doing ——

Ms. GARZA. So ——

Mr. HURD.—to prevent that from happening?

Ms. GARZA. There are a set of keys that—on the IRS that is only shared with the Department of Education. So as the applicant comes in and releases—tells us to release the data to the Department of Education, they don't have access. They don't have a key to de-encrypt that data. Only the Department of Education, once it gets to their side, that they will be able to de-encrypt the data.

Mr. HURD. Okay.

Ms. GARZA. So that applicant ——

Mr. HURD. So, Mr. Gray, how—you are responsible for FAFSA.gov.

Mr. GRAY. Yes, sir.

Mr. HURD. What are you doing to strengthen authentication if somebody has stolen credentials to actually authenticate it to the end-user?

Mr. GRAY. We are looking at several proactive measures to ——

Mr. HURD. We are looking portends that you are doing something in the future. Do you have a past tense verb that you can use on what you have done?

Mr. GRAY. For the Department, we follow Defense in depth and we have a whole series of actions that we're taking to ensure that we protect our systems.

Mr. HURD. And what are those series of actions?

Mr. GRAY. Some of them I referenced in my opening statement regarding data loss prevention, web access firewalls ——

Mr. HURD. So how does data loss prevention help with authentication?

Mr. GRAY. It would not. For authentication for FAFSA, the—this is the balance between—this is an application form where users are actually inputting their own data to gain access to apply for a student loan.

Mr. HURD. Yes, I get that. And ——

Mr. GRAY. So ——

Mr. HURD.—you have got to—it is your responsibility, right, to confirm that the person that is entering that data is indeed the person who owns the data. And I recognize this is a tough job, okay? I recognize that what you have to do is difficult. But you still haven't explained to me—we have proven and we have seen with the theft of over 100,000—or the impact on 100,000 students that the authentication mechanism within FAFSA.gov and the DRT tool is lacking. And my concern is that everybody is doing this. And I want to know what are you doing. And if there is not—if you need additional authorities to improve authentication on FAFSA.gov, I want to hear that, too.

Mr. GRAY. Thank you. The authorities that I have through FITARA has been very adequate. In terms of what we're doing, this is the balance between accessibility of the tool, which at this point is—it is a web application where students and prospective borrowers are coming in to apply. The level of authentication for that is currently set where it is so that we can cast the net as broadly

as we can to potential borrowers. The identity proofing piece comes in when we are dispersing the funds.

For the DRT, the challenge—or what we're doing is—we're looking at doing is masking and encrypting the data so that if an identity thief logs in through our system, they will not see that data, which would not allow them to exploit this vulnerability.

Mr. HURD. Madam Chairwoman, I apologize for going over my time.

Ms. FOXX. No problem.

Without objection, I am going to recognize Mr. Duncan for a unanimous consent request.

Mr. DUNCAN. Well, thank you very much, Madam Chair. I realize you are not going to be able to get to me for question and so I simply want to make a unanimous consent request to include in the record at this point an email from one of my constituents, a Melissa Macko, who is the financial aid administrator at the Tennessee College of Applied Technology because she has four good suggestion to help with this problem in her email. Thank you very much.

Ms. FOXX. Thank you, Mr. Duncan.

Ms. FOXX. Ms. Kelly, you are recognized for five minutes.

Ms. KELLY. Thank you, Madam Chair.

In recent years, hacking, identity theft, and cyber crimes have been on the rise. I have been the victim myself. Federal agencies have to do their part to secure their systems, but Congress must acknowledge the impact its own actions have had on the ability of agencies to protect their IT systems. Many agencies face serious challenges in modernizing outdated legacy IT systems and implementing stronger cybersecurity measures under severe budget cuts that have been imposed by Republican-controlled Congresses.

One of the agencies hit hardest by these cuts is the IRS. In May 2016, the IRS then-chief information officer Terence Milholland testified, and I quote, "the IRS budget system is the most critical challenge facing IT modernization."

Mr. CORBIN AND MS. Garza, what are the impacts of budget cuts on the ability of the IRS to modernize and secure IT systems? Are we putting taxpayers at greater risk?

Mr. CORBIN. So, Congresswoman, one of the things that Congress did do for us last year was appropriate the additional $290 million. We did take a portion of that funding to help us get the tools that Ms. Garza had described to help us identify and monitor our systems more closely.

We also continue to invest in the return review program or RRP, and so that allows us to create rules and filters so that as returns come in, we're able to evaluate those returns and then—for potential fraud or identity theft and then stop those returns before they are actually paid out.

Ms. GARZA. So I want—I think it's on. I want to thank Congress for the money that we did receive. That was extremely beneficial. It allowed us to put new technologies in place that are actually protecting our systems at a much higher level than we had done in the past. In this incident itself, we were able to address the situation a lot quicker than we would have an able to in the past be-

cause of the new monitoring capability and the data analytics capabilities that were implemented using those resources.

Ms. KELLY. And would you say more is needed or ——

Ms. GARZA. We would always be thankful for any additional resources and continued support in this area.

Ms. KELLY. To make us more secure?

Ms. GARZA. Yes.

Ms. KELLY. Okay. It is not just IT systems that have been affected by these resource lapses. Mr. Milholland testified last year that increased progress on systems modernization and cybersecurity measures, and I quote, "will require significant sustained additional resources in the IT area. Do you agree with that assessment?

Ms. GARZA. I would agree with Mr. Milholland's assessment of our needs.

Ms. KELLY. Mr. Corbin?

Mr. CORBIN. Yes, ma'am, I would agree as well.

Ms. KELLY. Okay. Yet again, Congress has failed to ensure that agencies have the resources they need to carry out their missions. For instance, under the IRS Restructuring and Reform Act of 1998, Congress gave IRS the authority to hire a limited number of individuals to staff critical technical and professional positions at salary levels greater than general schedule rates. This critical pay authority was intended to help the agency attract highly qualified individuals with advanced technical expertise who might otherwise be available for government service at normal Federal salary levels. The IRS used its authority to fill 168 of these positions from 1998 to 2013.

Does critical pay play a role in making Federal Government jobs more appealing to highly qualified technical individuals who may be interested in public service but could be earning a much higher salary in the private sector?

Ms. GARZA. Congresswoman, the critical—streamlined critical pay authority that we've had was extremely beneficial to the IRS. Because of that authority, we were able to bring on board high-level architects, engineers, and cybersecurity experts. Over the last several years, they have helped us ensure that we were doing what was needed to secure our perimeter and make sure that our systems were running much better.

The important component of this was the streamlined part of the critical pay. It allowed us to offer a job when we had—when we found somebody after the announcement was made and we identified somebody much quicker than the normal process would have been. A lot of times what we found was without the streamlined component, when we got back to the individual to see if they were still interested, the time had elapsed so long that we were not able—or they were no longer available or willing to come to work for us. So it is a critical component.

Ms. KELLY. But this pay authority expired in 2013 and has not been reauthorized, so American taxpayers lose when Congress ignores its responsibilities. Congress can and should swiftly pass streamlined critical pay reauthorization and act to provide adequate resource levels for cybersecurity at all agencies.

Thank you. Thank you, Madam Chair.

Ms. FOXX. Thank you, Ms. Kelly.

Mr. Issa, you are recognized for five minutes.

Mr. ISSA. Thank you, Madam Chair. And I look forward to the reauthorization if we can get the reforms that were required as of our last couple of hearings on the use of those 168 slots.

But let me go on to the actual data breach. Ms. Garza, under your interpretation of the data breach, this is a data breach, right? It is a major incident and it is a data breach. Is that correct?

Ms. GARZA. Under the definition of data breach it is classified as a data breach.

Mr. ISSA. Okay. So we have had a data breach. Let me turn it around for a moment because both you and Mr. Gray said that you had no—and I think Mr. Runcie all said the same thing. You had no information that personally identifiable information had specifically been compromised. That is pretty—paraphrasing all of you?

Ms. GARZA. That's correct.

Mr. ISSA. Okay. Well, I will go to IRS first. Ms. Garza, you were there for the kickoff of the Affordable Care Act website. And, as you know, in that website if somebody looking at their information at the top of the screen simply went up there and changed the State, they might actually look at somebody's personally identifiable information. That was a vulnerability that was discovered right in there in the HTTP line, right? Do you remember that?

Ms. GARZA. That was on the CMS site ——

Mr. ISSA. Right.

Ms. GARZA.—and so I don't have any detail ——

Mr. ISSA. Okay. Well ——

Ms. GARZA.—specifics on that.

Mr. ISSA.—just for historical sake, I actually did it. You could—and somebody did it themselves. You could simply change the State and you could end up with somebody else's identifiable information on your screen.

Now, they would have said that there was no breach, as Mr. Gray is sort of saying, because there was no proof anyone took that information and used it. But let me ask it another way. If you put a team of white knight hackers onto this vulnerability, could you have harvested information in your estimation?

Ms. GARZA. I think the evidence is that after the fact, yes, we—there were people that were accessing that application for bad reasons.

Mr. ISSA. Okay. So, Mr. Gray, I want to get you on the record under oath with an accountable statement. If there is evidence that people did nefariously gain some information, whether they used it or not, and that a team of white knight hackers or bad people could have harvested information, don't you have to admit that this is by definition a data breach, not just a hypothetical vulnerability but a vulnerability that was recognized that caused the shutdown of this tool?

Mr. GRAY. Thank you for the question and the request for clarification. I would say that when I am speaking about a data breach, I am speaking about the Department of Education's systems, and through our analysis, there was no Department data that was compromised or viewed through this. This was a case of unlawfully ob-

tained information that was used to go through our system to pull information from the DRT.

Mr. ISSA. Okay. But in this case we are talking about you together represent like an automobile, and you are saying that your right-hand wheel didn't come off but the left-hand wheel did or could have. Ultimately, the construction of the entire product was brought to a halt as a result of a failure, right?

Mr. GRAY. Yes, sir. Yes.

Mr. ISSA. Okay. And both of you—I just want to make sure because I heard Ms. Garza say it—but both of you admit that under FITARA, under the reforms, as CIOs, you have budget authority and the authority necessary to shut down or to make what changes are needed to control the security and accuracy of your work. Is that right?

Mr. GRAY. Yes, sir.

Mr. ISSA. Okay. So now my question to you in the short time remaining is, although this is about education and it is about the tremendous impact on students who will have a burdensome time applying, if we are to do the next level of reforms that this committee would be required to, if we have given each of you authority and one of you says I have got a breach and the other says I don't, how do we resolve—within the hierarchy of the executive office of the President so to speak how do we resolve making sure that the failure of the whole is in fact controlled by somebody? In other words, I am looking at the two of you. You gave slightly different testimony. I think you have come together on testimony.

But I want to know how in the future we do two things: one, make sure that somebody above you, sort of a super CIO, can make sure that this that this—that everyone—somebody is looking at the entire vehicle and not just a left tire and right tire; and then secondly, where were those white knights in this process? Where were the people who scrubbed this—third parties who scrubbed this data and system trying to find those vulnerabilities? Because somebody found it and it wasn't either of your teams. I will take an answer from either of you in the time that I am allowed.

Mr. GRAY. I don't know where those white knights were, sir. I do know that there were other entities within the government, USDS specifically, that was assisting with this as well. So I don't know where they were.

Mr. ISSA. Okay. So as Will said earlier, before the fact, you don't know. After the fact, of course, you could re-create it.

Ms. Garza, the two questions to you. You are very senior in this position. You have had a lot of experience. One, how do we bring together organizations like you that have become interdependent to make sure there is oversight of the entire combined authority? And two, how do we make sure there are white knights proactively in the future to try to find these things and maybe to concurrently and constantly try to find them?

Ms. GARZA. Congressman, we actually do have processes in place that—where we do penetration testing where we have individuals that come in and test our applications to ensure that they are not subject to white hackers coming in and getting away with the data.

Mr. ISSA. Although, white hackers I am okay with.

Ms. GARZA. White hackers, black hats ——

Mr. ISSA. Bad guys.

Ms. GARZA. So we do have that process in place and we do use it. I don't recall right now if that process was utilized on this application. It clearly should have, and perhaps we would have been able to avoid this.

As far as your other question, as the IRS continues to work with other agencies to provide data, it becomes more and more important that we actually address the concern that you have raised. I don't have an answer for you right now, but it's something we need to be very thoughtful about because I think this is going to start happening more often.

Mr. ISSA. Thank you. Thank you, Madam Chair.

Ms. FOXX. The gentleman's time is expired.

In the priority of the chair, I think will be helpful to this committee and to the Congress as a whole to get some sense of what kind of priority you put on testing your systems because it is pretty obvious that something like this should have been tested and should have been aggressively tested anytime you are sharing data with another agency. So I hope the committee will follow up on that.

Mr. Raskin, you are recognized for five minutes.

Mr. RASKIN. And Madam Chair, thank you very much.

Mr. Runcie, there has been a documented pattern of abuse with the student loan companies for many years now. Lots of scams have taken place. In 2012, the IG reported that a student loan company improperly accessed student borrower accounts to change the contact information of the borrowers in order to, quote, "make it difficult for the borrowers to be contacted by their loan servicers. Why would they do that? What is the scam? Can you explain to us how that works for them?

Mr. RUNCIE. Thank you. So they're commercial entities and they're fee-for-service entities, so they ——

Mr. RASKIN. These are legitimate businesses then? These are not internet scammers or ——

Mr. RUNCIE. They're not Internet scammers but the nature of the interaction between, you know, those entities and the students and borrowers, I can't characterize that. But they're businesses that are formed to provide commercial services, whether it's loan consolidation or something else.

It seems and it appears that in cases where they want to have a level of control to create a transaction or to continue through the process, they change email addresses and potentially mailing addresses and so forth to facilitate the process that they are taking the students and borrowers through.

Mr. RASKIN. But how do they profit from it? They take over the student's account?

Mr. RUNCIE. They—it's a—they may charge it—and I'm just going to make up a number. Let's say they charge $100 for consolidation or more. So there's an agreement that they will consolidate the loans and create a lower payment amount or whatever the agreement is, and they would be paid for that.

Mr. RASKIN. So did this actually take place? I mean, in one example the IG reported in 2013 that a company charged borrowers a monthly fee—I think it was $60—in order to put their loans into

forbearance with the promise of enrolling them in the Public Service Loan Forgiveness program eventually, which they weren't qualified for. But did that actually happen with people?

Mr. RUNCIE. My understanding is that it—there are these companies that provide these services, and a part of that process sometimes is they put people into forbearance with the understanding that they're ultimately going to go into consolidation. So those are third-party entities involved in a transaction that doesn't include the Department, you know, except for the fact that they're using the email addresses and the resources that we have to facilitate transactions where they make money. As ——

Mr. RASKIN. So just to get you straight there, they are using your website essentially as the framework to access their victims. Then, they prey on the people. But as far as you know, they might still be in this scam relationship with the students?

Mr. RUNCIE. Yes. We've looked at IP addresses and we've looked at some of the activity, and in some cases you will actually see loan consolidations. Whether it's 10 percent or 100 percent of their clients, we don't know. What we've stressed is user education to make sure people are aware that they can get these services done for free by leveraging resources that the Department provides.

Mr. RASKIN. Well, I get complaints on a daily basis pretty much from my constituents who feel like the whole system is a scam, but you are talking about a scam on top of a scam in a way. You are talking about people who are in serious debt from college and then some of these kind of low-riding companies are able to access them—charge them more money to offer them either real or completely illusory services, right?

Mr. RUNCIE. That's right.

Mr. RASKIN. Okay. Who is the ombudsman and champion of America's students and college graduates who is looking out for the scams in the IRS, the Department of Education, at every level of government? Is there anybody?

Mr. RUNCIE. I think we play a role. The Department plays a role. So, you know, for instance, I mentioned user education. The IG has noticed that this is an issue, and we're doing some things with our systems to make sure that we give them an additional tool or lever that they can use to prosecute, you know, bad entities. So, you know, we play a role in that and ——

Mr. RASKIN. How many prosecutions have there been since this was revealed?

Mr. RUNCIE. I don't have that information.

Mr. RASKIN. Have there been any prosecutions?

Mr. RUNCIE. I—the—we don't prosecute. It would have to be through the IG or some other ——

Mr. RASKIN. And let me just say I know everybody up there is working hard for the American people and has a tough job, but the overall institutional sense that I get is one of basic passivity and reactivity to events rather than getting on top of it. We have got millions of people who are carrying these loans. I think there is more student debt in America than there is credit card debt now. It is more than $1 trillion. And obviously, there is a lot of money being made there, including by people who are going out and preying on people who are already laboring under the burden of these

loans who—do we need to create an ombudsperson, somebody who is just a champion of the students and the graduates to make sure that they are not getting ripped off at every step of the process?

Mr. RUNCIE. Yes, I mean, we have an ombudsman, but it's not—it's sort of a pervasive all-inclusive person that sort of challenge—you know, challenges resources across government, across, you know, IGs, across operations. So, you know, that is potentially something that can be useful, but ——

Mr. RASKIN. Where is that ombudsperson located? Is that ——

Mr. RUNCIE. The ombudsman is located within FSA. They deal with complaints and issues that we can resolve. There are operational issues, so the customer service issues. They could be, you know, school-related issues. But in terms of ——

Mr. RASKIN. Did that person ever raise any of these issues with you about the scams being perpetrated on students through the website?

Mr. RUNCIE. No. Those scams are done by third-party entities that are outside of our scope. And so ——

Mr. RASKIN. So basically, it was nobody's responsibility to try to identify that threat? Is that right? I mean, that is not a gotcha question. I am just trying to figure out ——

Mr. RUNCIE. No, no ——

Mr. RASKIN.—to prevent this from happening again because, you know, there were cases of this going back four or five years now.

Mr. RUNCIE. Yes. The—again, the commercial entities that are marketing to students to provide services to those students and the students agree to, you know, obtain those services, and the questionable nature and value of those services is not something that we police. What we've been trying to do was provide user education and let people know that, you know, they don't need to use these resources. And we've—you know, working with partner organizations and so forth, but we don't have any control over those entities.

Mr. RASKIN. Thank you very much for your answers, and I yield back, Madam Chair.

Ms. FOXX. Thank you, Mr. Raskin.

Mr. Hice, you are recognized for five minutes.

Mr. HICE. Thank you, Madam Chair.

Mr. Corbin, do you have any idea how much the IRS loses to fraudulent tax returns each year?

Mr. CORBIN. No, Congressman. I can bring that back for you or go back and get that information for you.

Mr. HICE. Please do. But would it surprise you that in 2013 alone it was over $5 billion? Does that come as a surprise to you?

Mr. CORBIN. It does not come as a surprise, Congressman.

Mr. HICE. Okay. So it is no surprise that over $5 billion—let's just say that is the average year, $5 billion a year plus or minus in fraudulent returns—and now, as you—as has been clearly established, ballpark 100,000 taxpayers put at risk as thieves breach the DRT or—do you have any idea how many fraudulent returns resulted from those 100,000 taxpayers?

Mr. CORBIN. So, Congressman, what I know is that of the— we have received about 111,000 returns filed under those Social Security numbers. Of those returns, 80 percent of them were either

stopped by our filters prior to their refunds being paid or they were the actual legitimate taxpayer.

Mr. HICE. Well, that is good information, but that was not my question. I want to know how many fraudulent tax returns came from those 100,000.

Mr. CORBIN. Yes, sir. We have confirmed about 29,000 returns as identity theft.

Mr. HICE. Okay. And how many of those were fraudulent is my question. Commissioner Koskinen said it was about 8,000.

Mr. CORBIN. Yes, well, there are—so, Congressman, there are 8,000 returns that were not stopped by our filters that we have not been able to determine ——

Mr. HICE. That were fraudulent?

Mr. CORBIN. That we have not been able to determine if they were fraudulent or the legitimate taxpayer.

Mr. HICE. Okay. Well, that was my question. I would appreciate it if you would answer the question rather than run around it.

Mr. CORBIN. Yes, sir.

Mr. HICE. Do you have any idea how much money was lost due to those 8,000 fraudulent returns?

Mr. CORBIN. I believe that is about $32 million, sir.

Mr. HICE. It is about $30 million. Does the IRS reimburse the fraudulent tax returns from those who were victims?

Mr. CORBIN. So when a true taxpayer comes in and files a return, they do get their full refund that they're entitled to.

Mr. HICE. Okay. And who pays for that?

Mr. CORBIN. That comes out of the Treasury, sir.

Mr. HICE. So the taxpayers pay for it?

Mr. CORBIN. Yes, sir.

Mr. HICE. So we had $32 million just out of this 100,000 people, 8,000 fraudulent returns. So is that $30 million, does it include the reimbursement from the victims?

Mr. CORBIN. No, sir, it does not.

Mr. HICE. All right. So we are talking 60, $65 million in this one incident. We are talking if we have $5 billion a year in fraudulent returns, we are probably talking $10 billion that it costs the taxpayers every year after the victims are paid back. Does that ——

Mr. CORBIN. So of the 32, Congressman, again, we have not confirmed whether that is a fraudulent return or the true taxpayer.

Mr. HICE. Okay. I am just going by what Commissioner Koskinen said, and I would think that he would be accurate in that information.

Ms. Garza, I am still scratching my head over your comments earlier, that as far as you are concerned, you didn't know of any breach whatsoever, and yet it is pretty well confirmed there was a breach here and you even came back around and admitted that a little while ago.

Ms. GARZA. It depends on the timing, sir. In September we ——

Mr. HICE. It depends on whether or not anyone broke into the system. That is what determines a breach. And it just—I tell you, I just struggle. It appears to me at the end of the day—you are either in denial of what happened or you are incompetent or you are just untruthful in what is happening here. And I go back with what has been shared, too. The abuse that has been inflicted on

American citizens by the IRS is inexcusable and it is time that there is accountability and some change that takes place at the IRS. This is just—it is so bothersome it is indescribable.

Mr. Gray, let me come to you. It is my understanding that the Department may have the data retrieval tool operation for the purposes of income-based repayment plans back up in May or June. Is that correct?

Mr. GRAY. That is my understanding, sir.

Mr. HICE. Okay. That being said, if it is going—this has taken more or less three months to fix it, correct?

Mr. GRAY. Yes, sir.

Mr. HICE. Okay. If it has taken three months, why in the world was this not addressed last fall?

Mr. GRAY. Unfortunately, I can't answer that question because I am not involved ——

Mr. HICE. Who can answer that question?

Mr. GRAY. Mr. Runcie.

Mr. RUNCIE. It wasn't addressed—I think it's what we'd said a little bit before, which was we were making a decision at the time based upon the fact that there wasn't any criminal—material criminal activity. What the commissioner said was we would continue to monitor the situation, and once there was confirmed criminal activity, we would take the system down. So that was the focus of it, and then March 3 when there was—when we were contacted, the system was taken down.

Mr. HICE. The commissioner said that identity thieves used it to put forth false tax returns and made it clear that there was criminal activity, and that because of such, the system was going to have to be shut down. It looks like we are talking out of both sides of our mouth.

Madam Chair, I thank you for indulging me extra time. I yield back.

Ms. FOXX. Thank you very much, Mr. Hice.

Mr. Clay, you are recognized for five minutes.

Mr. CLAY. Thank you, Madam Chair.

And I find it deeply concerning that the Trump administration has started rolling back the protections that help ensure that students are not taken advantage of by predatory loan companies.

Mr. Runcie, Secretary of Education DeVos recently rolled back a critical protection put in place during the Obama administration. This protection prohibited loan servicers from charging up to 16 percent in interest on overdue student loans if borrowers entered a loan rehabilitation program within 60 days of default. Mr. Runcie, why did she rescind that protective order?

Mr. RUNCIE. I'm not aware—there was a policy memo that was rescinded. Is that what you're referring to, Representative Clay?

Mr. CLAY. Yes.

Mr. RUNCIE. Yes? So we—again, we're in the process of going through a competition for servicers, and the focus of that competition is to make sure that we have the best contract in place that's focused on high quality outcomes for students and borrowers. So that's what we're focused on. There hasn't been anything communicated from the Secretary that would change our ability to go for-

ward and to make sure that there's a vehicle in place to make sure that we optimize outcomes for students and borrowers.

Mr. CLAY. Now, doesn't that action place the financial interest of the loan companies over the interest of our students?

Mr. RUNCIE. That's not what we're doing, and that's not what's been communicated to us.

Mr. CLAY. Well, now, does it signal the loan companies that they can return to the predatory practices they engaged in before that take advantage of students? I mean, look, you and I know that people struggle to pay these student loans, so they came up with a way to give them some kind of relief, and now we are going to throw that out?

Mr. RUNCIE. No, I—look, I share your focus on making sure that we have the best circumstances for borrowers and students and, you know, if you look at income-driven repayment plans, which is a tool that was put in place to make it easier for students to manage their obligations and their debt, that has risen substantially. Our servicers and the Department is focused on making sure people get into plans that allow them to maintain ——

Mr. CLAY. Okay.

Mr. RUNCIE.—and manage their debt.

Mr. CLAY. Okay. Let's talk about those plans. Just last month, the Secretary withdrew another critical consumer protection afforded to student borrowers. Under the Secretary's order, contracts for debt collection will no longer be based on a loan company's history of helping borrowers but can again be based on a company's ability to collect debt. Can you explain why this change was made?

Mr. RUNCIE. Actually, the evaluation—and again, we're in procurement mode so there are certain things I can't talk about—but the actual evaluation does include looking at past performance and responsibility, as well as operational performance. So it is—the process is more than just looking at the ability to recover.

Mr. CLAY. Yes, but doesn't that go back to allowing these companies to pray on borrowers, I mean, and make that the standard operating procedure, that at all costs collect the debt?

Mr. RUNCIE. I can't speculate on that, sir.

Mr. CLAY. And, look, there have been troubling reports recently that the Department is reversing previous determinations that student loan borrowers qualified for a loan forgiveness program to encourage public service. Borrowers may have relied for years on these determinations to plan their educations, their careers, and their lives, and this program started in 2007. Under this program, borrowers can have the remainder of their Federal student loans forgiven after making 10 years' worth of payments if they serve full-time in public service jobs. Is that what is going on?

Mr. RUNCIE. Yes, I'm aware of the issue, and my understanding is that there is potentially some litigation around that. But, you know, the Public Service Loan Forgiveness is a vehicle that's out there. If you make payments for 10 years on time, you could be forgiven the remainder of that. That program is in place and we operationalize it.

Mr. CLAY. And are you intending on changing it?

Mr. RUNCIE. I'm not aware that there's any intention to change it. You know, that's an overall departmental perspective.

Mr. CLAY. It all comes down to let's scam these students, let's scam these borrowers, and let's take care of the servicers. And I think you should be ashamed of yourselves.

Mr. RUNCIE. Well, what I can say is that—and I can say this personally—is that there is a dedicated staff at the Department that's been there for quite some time, and our focus is not to facilitate or aid and abet any situation that compromises students and borrowers. We're committed to making sure they have the resources to be successful. We know it's difficult. It's a huge portfolio. But my intention is the same as your intention, which is to make sure that we don't have a structure that compromises any ——

Mr. CLAY. God help the borrowers.

Ms. FOXX. The gentleman's time is expired.

The ranking member is recognized for a unanimous consent request.

Mr. CUMMINGS. Thank you very much, Madam Chair. I want to just submit for the record a letter dated May 1, 2017, to the Honorable Kathleen Tighe just requesting certain documents with regard to this hearing.

Ms. FOXX. Without objection.

Ms. FOXX. The chair will recognize herself for five minutes.

I have to say that I agree with my colleague from Georgia who was here a few minutes ago that this situation of none of you all or people in your agency has been willing to take responsibility for what has happened. Either you are in denial or incompetent. I think the American people watching this are feeling the same way. I am troubled by my colleagues wanting to distract from the incompetence of the FSA and the IRS on display here today.

I want us to go after any bad actors outside the system, but our number one priority is to protect the American people. And everybody who works in this country is affected by the IRS. So, yes, we want to protect students from any unsavory characters, but all Americans are affected by the IRS if they file their taxes, and most of them do. Thank goodness we have a system where most people voluntarily do what they are supposed to do.

So the problem we have with our government agencies is there is no accountability for any of you individually, and that is a shame, a real shame on this country, that you all can ignore the continued incompetence and not be held responsible.

I do have some questions. The Department has taken some steps, Mr. Gray, Mr. Runcie, to mitigate the burdens on students' families and institutions caused by the DRT suspension, but I am concerned about the potential fraud the flexibilities you have put in place may cause. How is the Department protecting against fraudulent income reporting or ensuring that no new doorways to fraud are opened in this process? And I would like specifics, please.

Mr. RUNCIE. Well, in terms of—and thank you, Chairman Foxx—Chairwoman Foxx. In terms of specifics, you know, as you know, the verification—the backend verification is something that we've used along with, you know, the schools. So we do regression analysis and we come up with a formula that indicates a level of risk.

And so what we've done in terms of giving flexibility is we would reduce the lowest-risk element based upon a regression analysis so that even if we lessen the verification burden, it would be on a

risk-mitigated basis. So we would only eliminate the lowest-risk applicants potentially.

So the other part is that we're going to do this for a limited period of time, right, because we're going to get the tool back up October 1. And so for all the FAFSA cycles going forward, that won't be an issue. So it's somewhat of a temporary way to address the—to balance the burden to the schools against the risk to taxpayers.

Ms. FOXX. Mr. Gray, do you have anything to add to that?

Mr. GRAY. I would—yes, ma'am. I would say that there are also technical controls that we are looking at putting in place, and I would be happy to give more in-depth details about those controls specifically, but I would not want to reveal sensitive information right here.

Ms. FOXX. I understand.

So, Mr. Runcie, you touched on this a minute ago, that you are trying to get the system back up for the 2018 FAFSA filing period. Recognizing the balance between security and access, can you make the commitment to ensure there is no opportunity for the DRT to be misused again when it is once again operational? And I want to ask each one of you answer that question yes or no. Mr. Runcie?

Mr. RUNCIE. Yes, because the ——

Ms. FOXX. That is all I need to know.

Mr. RUNCIE. Okay. Yes.

Ms. FOXX. Mr. Gray?

Mr. GRAY. Yes, ma'am.

Ms. FOXX. Ms. Garza?

Ms. GARZA. I'm unsure.

Ms. FOXX. You are not sure?

Mr. Corbin?

Mr. CORBIN. I'm also unsure.

Ms. FOXX. Mr. Camus?

Mr. CAMUS. We will be watching closely.

Ms. FOXX. I think you have given the American people great confidence today from the IRS when you tell us you cannot secure the systems.

Mr. Runcie, I want to come back to you. I have been hearing troubling reports regarding the collection of defaulted student loans, and we have been hearing a lot about that in here this morning. Currently, struggling borrowers in default are without the critical services needed to rehabilitate their loans or access other benefits designed to lessen the impact of default. This is the responsibility of the Department. Can I get a commitment from you and the Department to provide my staff with critical information needed to assess the current loan default situation?

Mr. RUNCIE. Absolutely.

Ms. FOXX. And when?

Mr. RUNCIE. Two weeks.

Ms. FOXX. And when? Can we get—when will we know what the critical information is? When will you get that to us?

Mr. RUNCIE. So we can define what the critical information is within two weeks, and we could get you the information within a month because—so we'll have that to you within a month.

Ms. FOXX. Thank you for telling us that. We will hold you to it.

Mr. RUNCIE. Thank you.

Ms. FOXX. Mr. Connolly, you are recognized for five minutes.

Mr. CONNOLLY. I thank the chair.

I just want to say the breach at the Department of Education is something we have been warning about on this committee for quite some time. The Department of Education holds data on 139 million individuals. And I would echo what our colleague from Ohio, Mr. Jordan, said that the Department of Education may very well be in breach of law, and we are going to explore that.

However, what—Mr. Scott? I was just going to yield to Mr. Scott. Is he—all right. Sorry. Then I will pursue.

Mr. Gray, are you familiar with FISMA?

Mr. GRAY. Yes, sir, I am.

Mr. CONNOLLY. And what does FISMA require you to do, the Department of Education?

Mr. GRAY. To protect our information assets for the Department.

Mr. CONNOLLY. Well, that is not all it does. Doesn't it have a reporting requirement with respect to the legislative branch?

Mr. GRAY. Yes, sir, it does.

Mr. CONNOLLY. And what is that reporting requirement?

Mr. GRAY. Within seven days of an incident to report ——

Mr. CONNOLLY. And did the Department of Education comply with that seven-day reporting requirement?

Mr. GRAY. Sir, through our analysis of nearly 89,000 Social Security numbers, we did not identify that Department data was compromised in this situation. This was a situation where unlawfully obtained information was used to go through our system to access information through the DRT, which is why we did report it to US–CERT, and when it was identified that the compromise was through the DRT, we—that is when we did not report this as a major incident because our information—the information that the Department holds was not compromised.

Mr. CONNOLLY. And is that still your position?

Mr. GRAY. Yes, sir.

Mr. CONNOLLY. So from your point of view FISMA has not been triggered?

Mr. GRAY. A major breach of Department information was not compromised.

Mr. CONNOLLY. Is that the language of the law, that a major breach has to be compromised? That is to say a major breach has to lead to the compromise of data?

Mr. GRAY. No, sir. The—when the IRS reported this and we were notified on March 3, it was identified as an—the—an IRS system. It was not a Department of Education system. We did a thorough analysis of all of our system through FAFSA and nothing indicated to my knowledge that any of our information was compromised.

Mr. CONNOLLY. Mr. Camus, is that your view?

Mr. CAMUS. We have yet to determine the timeliness of the reporting of the incident, sir.

Mr. CONNOLLY. No, that is not my question. My question is do you concur with Mr. Gray that there was no breach of data?

Mr. CAMUS. We ——

Mr. CONNOLLY. Compromise of data?

Mr. CAMUS. We would view it as once somebody was able to see somebody else's data, that that in fact has been a breach.

Mr. CONNOLLY. I would, too, and therefore, I would argue FISMA is triggered. Would you agree?

Mr. CAMUS. Yes, sir.

Mr. CONNOLLY. Well, Mr. Gray, it sure does sound like you are splitting hairs and you are coming up with a criterion that was not envisioned in the law itself, nor was it reflected in the language of the law itself. I mean, we don't have traffic laws that allow you to decide, well, I didn't hurt anyone. Yes, I was speeding, but I didn't hurt anyone, so therefore, I shouldn't get a ticket. I mean, the law is there to make sure that the legislative branch is informed in a timely fashion when this kind of activity occurs. And the reason isn't so that we are keeping score. It is to make sure that we are doing what we can on our part to protect sensitive data of American citizens.

And it seems to me that it was incumbent upon the Department of Education to inform us in a timely fashion. In fact, I would even argue if I were managing the Department of Education, you know, the better part of wisdom would dictate that I inform them even if I didn't believe FISMA was triggered.

But the fact that months could go by and, as Mr. Camus just said, a breach is a breach. Once it is breached, you have to assume that data is compromised, if not today, tomorrow, because it can be. And I just don't find your explanation very credible, and I frankly think it is a disservice to, you know, the people whose data you possess. And it is an end around with respect to the legislative branch, and I think it is in violation of the law.

I know we are going to pursue that more, but I don't think that is something that puts the Department of Education in any kind of good light.

My time is up. And I am sorry I missed Mr. Scott. I was going to defer to him. I thought I was being asked to.

Thank you, Madam Chairman.

Ms. FOXX. Thank you, Mr. Connolly, and thank you for honing in on the issue of the day and looking for what remedies we might have under the law.

Mr. Meadows, you are recognized.

Mr. MEADOWS. Thank you, Madam Chairman.

We are going to follow up, Mr. Gray, right now, because I can tell you that Mr. Connolly is spot on. And this is not your first rodeo. You know, we have had these other issues before with regards to privacy. And is it your sworn testimony today that this did not actually require notification of Congress?

Mr. GRAY. No, sir. My understanding is that the IRS had reported the incident and that it was a breach, but the Department of Education, my understanding when I was notified on March 3 that the notification had already happened. I have learned in this hearing that it did not happen.

Mr. MEADOWS. Well, how can the American people, actually people who share private information with you who expect it to be protected have confidence when you are here today and you don't even know the full story, that you are finding it out in a hearing when you knew that we were going to be looking at this?

How can you find a hacker who truly wants to come in and do harm and you can't even be prepared for sworn testimony today on questions that I presume that you knew we were going to ask?

Mr. GRAY. I understand, sir. The challenge ——

Mr. MEADOWS. Where is the outrage? Where is the outrage, Mr. Gray? Are you not outraged?

Mr. GRAY. I absolutely am. Our ——

Mr. MEADOWS. Why didn't you notify Congress?

Mr. GRAY. My understanding was this was not a Department of Education ——

Mr. MEADOWS. Well, you realize that was not—did you have your counsel that said you don't have to notify us? Who did you check with who said you don't need to notify Congress?

Mr. GRAY. We went through our incident response process, who did an assessment ——

Mr. MEADOWS. So why did you refer something to an outside agency before you notified your own IG within your Department?

Mr. GRAY. Our IG was notified right after we ——

Mr. MEADOWS. Well, but according to my documents, you actually notified US–CERT first, according to your testimony. Why would you do that and wait to get the IG involved?

Mr. GRAY. Because when we notify US–CERT, it's to let them know that we were investigating something that had occurred. At that time, we weren't sure what had happened.

Mr. MEADOWS. Okay. So the IG, you go, you notify the IG. It was important enough to notify the IG but it was not important enough to notify Congress?

Mr. GRAY. Hindsight, sir, yes, it was important enough to notify Congress.

Mr. MEADOWS. Well, at what point are we going to get this right? Because we continue to have breaches. Mr. Connolly and I have had a number of hearings where we have raised this as a concern, and yet what happens is is we are always coming in after the fact to look at this. Do you not see a problem with that?

Mr. GRAY. I do see a problem with that.

Mr. MEADOWS. Well, when are we going to get it fixed?

Mr. GRAY. Sir, we receive on average more than 1.5 million intrusion attempts every single month at the Department, and what my team does is we assessed to determine whether or not something had happened, nothing happened, and logistically—I mean, I know in this case it's easy to look and say, okay, this should have been reported. I understand that.

Mr. MEADOWS. So you're saying it's a matter of logistics on why you didn't report it? Because that's different than what you said earlier. Earlier, you said you didn't think you had to report it.

Mr. GRAY. Based on the analysis that my team did, we—our information, the information that I am—that our ——

Mr. MEADOWS. So how confident are you that there was only 89,000 people that were affected?

Mr. GRAY. Based on the logged analysis that was done at the Department, very confident.

Mr. MEADOWS. All right. A 10?

Mr. GRAY. Yes, sir.

Mr. MEADOWS. So if we find out there is more than that, are you willing to resign?

Mr. GRAY. If it's—if I don't know the information, no, sir. I mean, from what I have ——

Mr. MEADOWS. Well, you said you are confident at a level of 10, so I guess I would stake my reputation on that if you were confident at a 10. So if there is more than that— because the IRS knows that sometimes we find out that there is actually more people that were affected than was originally thought. So if you are confident at a 10, are you willing to stake your reputation and your job on it?

Mr. GRAY. So, sir, the challenge here is that when we ——

Mr. MEADOWS. Sir, I am representing people back home in North Carolina, as every member here is, and you know what, they fail to realize that you can't protect sensitive information that they give you, and they don't understand that. I don't understand it. At what point are we going to have the confidence when people share their information with the government that it is not subject to being shared with another party? Isn't that what your job is all about as CIO?

Mr. GRAY. Yes, sir.

Mr. MEADOWS. All right. The next time, are you going to inform Congress when there may be a doubt? Will you inform us within the seven days?

Mr. GRAY. Absolutely.

Mr. MEADOWS. All right.

Ms. Garza, last question to you. Why didn't you inform us?

Ms. GARZA. Congressman, we briefed the staff shortly after we brought down ——

Mr. MEADOWS. You didn't brief our staff. Why didn't you inform Congress? That is the question of the day. Because according to your TIGTA, it is 100,000, so it is certainly—even meet the threshold, but why wouldn't you inform us?

Ms. GARZA. So, Congressman, we did inform the Congress that this was a data breach. The reason why it took as long as it did is because we were going through analyzing the information. The initial population was much smaller than 100,000 that we thought were impacted. We also needed to coordinate with the Department of Education to determine whether ——

Mr. MEADOWS. But didn't you find it just based on dumb luck? It was actually just one of your IRS employees that actually got a transcript request and they said, hey, something doesn't smell right here?

Ms. GARZA. Congressman, we have multiple layers of ——

Mr. MEADOWS. That is not the question. Wasn't it dumb luck that you happened to find this?

Ms. GARZA. No.

Mr. MEADOWS. So it wasn't an IRS employee that happened to get a transcript? Be careful; you are under sworn testimony here.

Ms. GARZA. The—it was an IRS employee. He received a notification as part of one of our defense mechanisms that his account had been accessed.

Mr. MEADOWS. So it was an IRS employee who happened to have his stuff that was notified and we said, hold on, we got a problem here? Do you not see that that is almost laughable?

Ms. GARZA. One of our mechanisms to determine whether something has gone wrong is a notification to the taxpayer. Our systems automatically send out a notification ——

Mr. MEADOWS. So you purposely embed IRS employees in all this so that they might get a personal notification so they can highlight this? Come on.

I will yield back.

Ms. FOXX. The gentleman's time has expired.

Mr. Sarbanes, you are recognized for five minutes.

Mr. SARBANES. Thank you, Madam Chair. I thank the panel.

Ten years ago, I was proud to lead the effort here in the House and we teamed up with Senator Kennedy on the Senate side to create the Public Service Loan Forgiveness program. And we have paid close attention to that over the last 10 years, working with U.S. Department of Education along the way, to create online resources to help borrowers understand whether they are going to qualify for this program, which includes reduced monthly payments, as well as ultimate forgiveness of their outstanding principal if they commit 10 years to public service.

That includes the need to be assured that the employment you have, the particular employer that you are working for, qualifies under that public service category and that you can count the time spent with that employer towards your 10 years and ultimately earn the forgiveness.

Congressman Clay alluded a moment to go to the fact that there is some troubling position that the U.S. Department of Education has been taking over the last 18 months with respect to certain categories of employers. They are now telling borrowers who relied on an assurance that that employer would qualify, being told now that it won't, and there is some litigation around that, Mr. Runcie, as you indicated. And we need to get to the bottom of that because our borrowers that have relied on assurances that have come from the Department and they need to be able to count on that. Otherwise, the rug is being pulled out from under them.

I know that some of us here have been trying to get a briefing from the Department over the last few weeks. That has not yet happened. Could you commit to us today that the Department would be willing to brief us on this issue and what is happening with that?

Mr. RUNCIE. So I—it's not just FSA. I mean, we obviously operationalize it and we put the resources out there so people can avail themselves of Public Service Loan Forgiveness. But I think that briefing would include other entities such as ODC and policy, some other folks. I can't ——

Mr. SARBANES. Well, that is fine. Can you help us arrange to get that briefing done and get it done quickly so we know what is happening with this and then we can take appropriate steps in our oversight capacity?

Mr. RUNCIE. Absolutely. It is an important issue, and I think we're real focused on it, so I will absolutely commit to working, you know, with my colleagues to ——

Mr. SARBANES. Now, let me stay focused on the Public Service Loan Forgiveness piece and loan-driven repayment, because when you talk about the universe of borrowers out there that are impacted by the breach that we are talking about today, using this data retrieval tool, you have the part of that universe that are folks that are, you know, involved with standard repayment, and then you have those who are in a loan-driven repayment situation based on one program or the other. That includes Public Service Loan Forgiveness. And they have to be handled differently because they are impacted differently.

And you have indicated that with respect to the standard repayment world that you are going to try to get this tool back in service by the beginning of the next year, so October is the goal. But with respect to loan-driven repayment, you are trying to get that back up by May.

So can you tell us how confident you are that—I mean, it is May now. I mean, how confident are you that that is going to be available to folks that are benefiting from loan-driven repayment arrangements? Is that going to happen?

Mr. RUNCIE. Yes, we are very confident. You know, as the IRS mentioned, they've completed the encryption part, and we have a timeline that gets us to a place where it's up and running by the end of this month. So we know it's only another few weeks but we can commit to that.

Mr. SARBANES. I appreciate that. Could you also let me know—I know one of the remedies or sort of stopgap remedies when someone is in a situation perhaps not being able to access a tool that allows them to do things in a timely fashion is forbearance for, you know, two months, three months, what have you. That can work okay for the standard repayment folks because there is really no downside to losing a couple months in terms of your repayment.

But if time is of the essence in the sense that you are accruing time towards this 10-year repayment period, then forbearance isn't necessarily going to be a great solution for people that are in the loan-driven repayment category. Is that something that the Department has considered, and is there a way to provide a remedy there that doesn't complicate the lives of these folks that are in a particular program like that?

Mr. RUNCIE. Yes. I'll make sure that we are—I know we're considering a lot of different issues around it, and I believe that's one, but we'll certainly make sure that we're focused on that because I do understand the issue around that.

Mr. SARBANES. Okay. I yield back.

Mr. RUNCIE. I wanted to add one thing, and we're pretty firm on the end of May unless potentially some requirements change, but I think we're committed to the end of May for the tool being back up for the income-driven repayment plans.

Ms. FOXX. Well, thank you, Mr. Sarbanes.

Thank you, Mr. Runcie.

Mr. Mitchell, you are recognized.

Mr. MITCHELL. Thank you, Madam Chair.

I join your dismay that rather than discuss the data breach, the impact it has on the ability of students to get assistance, how we deal with the data breach going forward, avoided that some wish

to talk about issues that we are now going to investigate as well, which is potential bad actors to obfuscate with the current issue is, which is the IRS and the Department of Ed's inability to have this tool work and not have it breached but rather talk about other issues.

We only have so much time here. We only have so many things we do simultaneously. Let's talk about the issue we put on the table. So I am dismayed, and I guess I shouldn't be surprised.

Mr. Connolly, you have—I am sorry, Mr. Gray. You have seen the Wizard of Oz, right?

Mr. GRAY. Yes, sir.

Mr. MITCHELL. Did you see the part where they talk with the scarecrow and they ask him which way the yellow brick road is? Do you remember that part?

Mr. GRAY. Yes, Representative.

Mr. MITCHELL. And the scarecrow goes like this? Do you remember that part?

Mr. GRAY. Yes, sir.

Mr. MITCHELL. In my opinion, frankly, sir, that is exactly what you are doing when you talk about, well, the data breach happened at the IRS and we didn't think it was us so we didn't need to worry about notification. You know, when you have got something as sensitive as personal information for the number of students that you have, the moment in time that you think your data has been breached, you have a legal if not moral—moral if not legal responsibility to notify Congress. That is a lot of information. And it wasn't done.

And it is not the first time it wasn't done. And I don't understand that. And I don't know how it is we get across to the Department that that is your responsibility by law if not morally. What does it take to get someone to understand that over there? Can you explain that to me?

Mr. GRAY. I have committed that going—that I will do that, sir.

Mr. MITCHELL. I ran a private career school group that had 6,000 students a year, close to 7,000 students a year for six-and-a-half years as a CEO. Ms. Garza, do you know what— the CIO reported to me for a reason. Do you know the deal I had with the CIO if we got hacked? And we didn't have as many hack attempts is the Department of Ed, I will just be honest about it. Do you know what the deal was? Do you want to guess what the deal was if we got hacked?

Ms. GARZA. You held the CIO accountable.

Mr. MITCHELL. The CIO's resignation was on my desk. That is how sensitive that information was. And I am serious. I am absolutely serious. I will give you his phone number. You can call him. His resignation was on my desk. His cell phone got buzzed any time there were certain sets of activities, whatever hour of the night.

Now, who on your staff gets called in the middle of the night or gets a buzz if in fact data goes out of whack? Anybody?

Ms. GARZA. The CISO is the first one that gets a call, and then depending on the type of breach, she will call me.

Mr. MITCHELL. Let me change the subject for moment here because time is limited. I have heard repeatedly budget concerns,

budget concerns. I come from the private sector, and I am absolutely amazed. The first time a problem comes up, everyone wants to whip out the taxpayers' checkbook because, hey, just spend more money. From the world I come from, we first identify the problem and what it takes to solve it and not just throw money at it.

So answer a question for me, Ms. Garza. And by the way, I mean, we all know how many people have had their data hacked, false tax returns. I had it happen to me. My youngest son is dealing with it right now this year. How much money do you need to tell this group, to tell Congress that you can secure this system? Exactly how much do you need in your budget that you will put your letter of resignation there if you get hacked? How much money?

Ms. GARZA. I don't know how much money it would take.

Mr. MITCHELL. But you ask for more money all the time.

Ms. GARZA. We ask for additional resources to continue to fortify ——

Mr. MITCHELL. Every year.

Ms. GARZA.—our systems.

Mr. MITCHELL. Every year.

Ms. GARZA. That's correct.

Mr. MITCHELL. I asked you a question. How much money do you need in your budget for data protection that you will put that budget request in and simultaneously you will tender your resignation that if you get hacked, you go home?

Ms. GARZA. I don't have that dollar amount in my mind. What I do know is that criminal enterprises are constantly changing ——

Mr. MITCHELL. Oh, I understand that.

Ms. GARZA.—and their tactics, and so to make the statement that we can guarantee a system is secure quite frankly is a little bit folly. We are doing everything that we can to make sure that our systems are secure. We have not had a breach of our internal systems, although we have had data loss. And so to put—to try to come up with a dollar amount that would guarantee that something will not occur I think—at that point I would think that we are probably not going to end up being secure.

Mr. MITCHELL. And my time is expiring and I appreciate the patience. Anywhere else in the world in the private sector at least somebody says we really screwed up here. At least someone says, well, hey, we missed—you know, they take accountability for it. My technology staff took it personally when someone tried—you know, when we had people trying to hack it, when we had—how we secured it. It was the game. It was their life. And the fact that folks can sit here and say, well, basically, stuff happens. But when you are talking about people's information to the Department of Education or IRS, it is not just stuff happens. This is their life. It is their tax return. It is their personal information used to get credit elsewhere.

This is not minor stuff, and I don't see the perspective or concern that, well, we do the best we can. If it is wrong, we may notify, we may not notify. We may not think it is our problem because it is the IRS's problem. Again, they went that way. Somebody needs to be accountable for it, folks. And I will join Mr. Connolly and others in finding a way we have got to hold folks accountable because

we can't have this kind of data leaking out, people taking it and using it for adverse purposes. You should be ashamed.

I yield back. Thank you.

Ms. FOXX. The gentleman's time has expired.

Mrs. Maloney, you are recognized for five minutes.

Mrs. MALONEY. Thank you, Lady Chair.

We need to do everything we can to prevent cyber attacks from occurring, but when they do occur, it is critical that we take it as seriously as the gentleman said and also that we learn from them.

In 2015, criminal elements attacked the IRS and its Get Transcript application, the tool that allows taxpayers to obtain copies of prior tax returns using a collection of personal information. An organized crime syndicate accessed this application using stolen personal information of individuals and obtained tax data for a staggering 300,000 individuals. Is that correct, Mr. Corbin?

Mr. CORBIN. That is correct, Congresswoman.

Mrs. MALONEY. And since that incident, the IRS has been working diligently to increase the security of its systems. In January 2016, a result of cybersecurity improvements, the IRS stopped an attempt to acquire the e-filing PIN number of taxpayers. Mr. Corbin and Mrs. Garza, is that correct? And can you describe what the improvements were that were able for you to stop this other attempt?

Mr. CORBIN. So for—so, Congresswoman, for Get Transcripts, we took that application down and did an assessment level of risk, and we put in place what we call secure access authentication. It is a higher level of authentication that requires ID proofing, financial verification, and then an activation code in order to be able to get access to your transcript.

We continue to take the dollars that were provided by Congress, the $290 million, to invest in additional cyber tools that allowed us in this case to be able to detect when there was activity occurring on tools that we have that are outside the IRS network.

For the e-file PIN, Congresswoman, we looked at that and again identified that that would be a vulnerability. The e-file PIN application is not back up. We eliminated the e-file PIN application and now require AGI or the self-select PIN, which taxpayers have.

Mrs. MALONEY. Okay. After the 2015 incident, you did a reassessment of the security of all of your online applications, including the data retrieval tool. And as you stated in your testimony, that assessment—and I am quoting from your testimony—indicated the need for strengthened procedures and led to collaboration with the Board of Education to best implement those procedures. Now, is that correct?

Ms. GARZA. That is correct.

Mrs. MALONEY. Okay. Now, I want to turn to the 2017 data retrieval tool incident where criminals were able to use personal information gathered elsewhere to create student aid accounts on the Department of Education's websites and obtain individuals' sensitive tax information. So, Mr. Corbin and I would say Mrs. Garza, is it right to say that, much like in 2015, individuals were seeking the information necessary to file fraudulent returns?

Ms. GARZA. That's correct.

Mrs. MALONEY. Yet this time, individuals were much less successful in obtaining the returns, and according—would you like to comment on that?

Mr. CORBIN. No, Congresswoman. Go ahead.

Mrs. MALONEY. According to GAO, identity theft at the IRS has decreased in recent years because the IRS has improved its ability to detect fraud before processing returns. This approval detection ability is illustrated by the fact that automatic security filters were able to stop almost 65 percent of potentially fraudulent refunds from being issued in the data retrieval tool incident. Is that correct?

Mr. CORBIN. That is correct.

Mrs. MALONEY. So we can't stop all cyber attacks. That is just the reality of today. But we can learn from them. So I think you have shown your ability to do that.

So, you know, when you file—why would somebody want to file a fraudulent return? What was the purpose of it for the purpose ——

Mr. CORBIN. So, Congresswoman, most people file fraudulent returns with the hopes of obtaining a refund ——

Mrs. MALONEY. Whoa, okay.

Mr. CORBIN.—from that return.

Mrs. MALONEY. And are they successful?

Mr. CORBIN. Congresswoman, fraudsters are successful, but we have gotten so much better over the years. The IRS has a public-private partnership called the Security Summit where we work to protect the tax ecosystem, working with State Departments of Revenue, with software developers so that we can build better systems to help protect the tax ecosystem.

As you stated in this case with the data retrieval tool, we have new data elements or information that we are using in our filters. It did allow us to stop 80 percent of the returns that were filed in this event that were either potentially fraudulent or before the refunds were able to be paid.

Mrs. MALONEY. Well, thank you. My time is expired, but I hope we can continue to fund the IT improvements that the IRS requests so we can continue going forward in being more effective in stopping fraud and helping taxpayers.

Thank you for your testimony today.

Ms. FOXX. Thank you, Mrs. Maloney.

Mr. Grothman, you are the one we have been looking for, the last one.

Mr. GROTHMAN. Good.

Ms. FOXX. You are recognized for five minutes.

Mr. GROTHMAN. Mr. Gray, I will give you a few questions. How long have you been the chief information officer over at Education?

Mr. GRAY. Eleven months, sir.

Mr. GROTHMAN. Okay. And since November of 2015, this committee has uncovered what we feel are significant shortcomings in your IT security plans before you were even there, as well as corruption of the former CIO. As newcomer, what concerns you the most, and what were your first actions as CIO to clean this up?

Mr. GRAY. There were several—I had five focus areas when it came to the Department. One was on security, another was

FITARA and organizational health, so there were policy challenges. There was numerous things that we need to improve. And I will say in the last 11 months we have made significant progress at the Department in terms of implementing processes, implementing policies, changing personnel.

Mr. GROTHMAN. Okay. Last year, US–CERT reported 192 incidents in your Department. Can you tell us what information leaked out in those 192? Give us, say, how many files and what they covered?

Mr. GRAY. I would have to get that information for you, sir. I do have a list of the information and—but I'd want to verify.

Mr. GROTHMAN. Give me a broad—you know, there must be some that stuck in your mind. What are the type of things that get out there?

Mr. GRAY. Typically, Social Security numbers that were inadvertently sent from one individual to an individual it wasn't supposed to or it wasn't encrypted.

Mr. GROTHMAN. Anything beyond that? Any information connected with the Social Security numbers?

Mr. GRAY. I would—I'd want to verify, sir, but to my knowledge I would ——

Mr. GROTHMAN. You can't think of any example?

Mr. GRAY. Not at this moment.

Mr. GROTHMAN. Okay. Is this—I guess we will call this OCIO–14 handbook?

Mr. GRAY. Yes, sir.

Mr. GROTHMAN. Okay. You know how recently this was updated? Or I've got one that I believe is right now the current one that you must give your employees. Do you know how recently it was—or how recent the most recent update was?

Mr. GRAY. There is a draft going—circling right now to—that is being updated, that has been updated and that is being routed for concurrence right now.

Mr. GROTHMAN. Yes, but do you know how long—how old this is?

Mr. GRAY. Several years, sir, too many.

Mr. GROTHMAN. A little over six years now. Okay. Do you think that is satisfactory?

Mr. GRAY. No, sir.

Mr. GROTHMAN. Okay. Could you give us a hard number as to when you feel you have got something new available for your new employees?

Mr. GRAY. For OCIO–14?

Mr. GROTHMAN. Correct.

Mr. GRAY. The concurrence process within the Department takes an amount of time, so I can't comment on that, but I will say that I have a solid draft that is going through concurrence right now.

Mr. GROTHMAN. Can you give us a guess? A month, four months, a year?

Mr. GRAY. My understanding is the process is about six months to a year to go through formal concurrence.

Mr. GROTHMAN. And how far are you through the process now?

Mr. GRAY. We started last week. We started the actual concurrence process last week, sir.

Mr. GROTHMAN. Okay. So you began something but it could be a year before we get something that is more than six years old?

Mr. GRAY. I will expedite it because I know it's critical to the Department.

Mr. GROTHMAN. And critical to us and critical for the public.

Could you give us—when we talk about the files with the Social Security number, can you tell us what else is in those files?

Mr. GRAY. I would have to look specifically at them. I— at this point—I mean, sometimes they're Excel spreadsheets that contain Social Security numbers. I would have to look to verify.

Mr. GROTHMAN. Okay. I will try Mr. Runcie. Have there been breaches of your ——

Mr. RUNCIE. Not to my knowledge, no. There was I think about—it might've been four years ago there was a time where the system was open for a few minutes, and there were 6,000 cases of information that was viewed that shouldn't have been viewed, but that was the only systemic breach or exfiltration of—it wasn't even an exfiltration but it was an incident that occurred at that time.

Mr. GROTHMAN. How long ago was that? How long ago was that?

Mr. RUNCIE. It was a few years ago. I'm not exactly sure.

Mr. GROTHMAN. So you have had nobody breach anything for the last four or five years, do you think, three or four years we will say?

Mr. RUNCIE. Well, there has been no material breach. There is a possibility that there might have been an incident here or incident there in terms of student aid data but none to my knowledge.

Mr. GROTHMAN. Okay. They don't tell you?

Mr. RUNCIE. I would be informed if there was, and I'm not aware of any.

Mr. GROTHMAN. Okay. I yield the remainder of my time.

Ms. FOXX. Thank you very much.

I am ready to close. I have none of my colleagues on the Democrat side, so I will make some very brief comments.

To not broach our protocol, I will not ask questions, but I will let Ms. Garza, Mr. Corbin, Mr. Camus know that we will be asking you exactly how many fraudulent returns were filed as a result of the breach and when those people obtained that information. And we will want an answer in what most of us would consider reasonable time.

It has been extraordinarily difficult today to get any kind of specific answer out of any of you. And I think Mr. Mitchell's comments about the scarecrow were entirely apt. You are blaming each other. The American people frankly are tired of this kind of display of incompetence again. You all cannot answer questions or will not answer questions. It is a little difficult to know.

And let me tell you something. In my world, $30 million is a lot of money, a lot of money. And you all don't seem to take it seriously at all, that as a result of your not being able to take action when a breach is made and you are not following the law to let Congress know, it is even more troubling to me that you take so long to do anything.

Mr. Grothman's comments about a document that is very important taking seven years to update, it is pure incompetence.

And I would venture to say that we might be able to get better people coming into your agencies to do the work that needs to be done regardless of the pay if they thought they could get something done. But the bureaucracies are so impossible to change.

And I do want to note that both Mr. Gray and Mr. Runcie came to the Department and all of you all, too, in the IRS under the Obama administration. Our colleagues are going to raise Cain with the existing Departments and make it appear as though this is the responsibility of the current administration. And I think it needs to be made abundantly clear that you all came into these agencies under the previous administration and have been kept on by the previous administration.

We will also put into the record the expanded timeline in terms of when these problems began occurring and point out where we possibly can the inaction of the people who are supposed to be working for the American people and keeping their data confidential.

So I thank you all for being here today, and this hearing is dismissed.

[Whereupon, at 12:07 p.m., the committee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

NATIONAL ASSOCIATION OF STUDENT FINANCIAL AID ADMINISTRATORS
1101 CONNECTICUT AVENUE NW, SUITE 1100
WASHINGTON, DC 20036-4303

Statement
of
Justin S. Draeger
NASFAA President

Submitted to the
U.S. House of Representatives Committee on
Oversight and Government Reform

"Reviewing the FAFSA Data Breach"

Testimony: Justin Draeger, NASFAA

On behalf of the National Association of Student Financial Aid Administrators (NASFAA), we submit the following statement for the record with respect to the recent outage of the Internal Revenue Service (IRS) Data Retrieval Tool (DRT) and its impacts on students applying for federal student aid using the Free Application for Federal Student Aid (FAFSA) and on federal student loan borrowers applying for or renewing eligibility for Income-Driven Repayment (IDR) plans. NASFAA represents financial aid administrators at 3,000 public and private colleges, universities, and trade schools across our nation. Collectively, NASFAA members serve 90 percent of undergraduate students studying in the United States.

Since its inception eight years ago, the IRS Data Retrieval Tool has become the cornerstone of federal financial aid simplification, with students and institutions of higher education relying on its efficiency for both the application and verification processes. The abrupt outage in the midst of the application filing season is extremely troubling, made worse by the fact that it took the Department of Education (ED) and the IRS nearly a week to publically acknowledge that the tool was not working.

NASFAA first received reports from member institutions of the DRT outage on March 6, 2017. In response to those reports, NASFAA reached out to ED staff who confirmed verbally that the DRT had been down since March 3 due to technical issues. On March 9, nearly a week after the outage took place, ED and IRS issued a joint statement[1], the first public acknowledgment of the outage. This statement indicated the cause of the outage as an IRS decision to suspend the DRT due to concerns that the tool could be misused by identity thieves, and anticipated a timeframe of several weeks for the DRT to become functional again. Also on March 9, Rep. Lloyd Doggett (D-TX) issued a letter[2] to Education Secretary DeVos and IRS Commissioner Koskinen urging prompt investigation and resolution of the DRT outage, a timeline for resolution, and collaboration with institutions of higher education to ensure financial aid applicants were not penalized for missing deadlines due to the DRT outage.

On March 14, NASFAA - in partnership with several other partnering organizations - sent a letter[3] to Secretary DeVos and ED Chief Operating Officer Jim Runcie requesting that ED update its communications and instructions to reflect the DRT outage, allow applicants to use paper tax return copies to satisfy verification requirements in place of IRS tax transcripts, revise verification selection criteria to provide a more generous

[1] https://www.ed.gov/news/press-releases/internal-revenue-service-irs-and-us-department-education-office-federal-student-aid-fsa-statement-about-irs-data-retrieval-tool-drt
[2] https://www.nasfaa.org/uploads/tn/doggett_irsdrt.PDF
[3] https://www.nasfaa.org/uploads/documents/NASFAA_DRT_Letter.pdf

tolerance to keep the number of applicants selected for verification stable, and to expand the tolerance for required school resolution of cross-year conflicting information.

On March 16, House and Senate leaders sent a letter[4] to ED requesting a briefing on the DRT outage within one week. That same day, the House Committee on Oversight and Government Reform and the Committee on Education and the Workforce sent letters to both ED[5] and IRS[6] requesting briefings. On March 30, a second joint ED-IRS statement[7] was issued, this one providing more information on the rationale behind the outage, stating that identity thieves may have used personal information to access the FAFSA as a means of obtaining tax information from the DRT to file fraudulent tax returns. The statement indicated that IRS was working to identify the number of taxpayers affected by questionable use of the Data Retrieval Tool. In this statement, the timeline for the DRT to be made available was revised to the start of the next FAFSA season (which is October 1, 2017). Included in this statement was guidance that federal student loan borrowers applying for or renewing Income Driven Repayment (IDR) plans, who also use the DRT to verify their income, could submit paper tax returns as income documentation.

Finally, on April 24, nearly two months after the DRT outage was discovered, ED issued guidance[8] to institutions of higher education that they may accept paper copies of tax returns or signed statements of nonfiling in place of IRS tax transcripts to satisfy verification requirements, action that was very well received by institutions once it was finally released.

It must be noted that the DRT outage is especially harmful in this first year of "Early FAFSA" and prior-prior year (PPY). Before this year, the FAFSA became available on January 1, and applicants were asked to provide income information from the prior tax year. For the 2017-18 application year, the FAFSA became available three months earlier, on October 1. This "Early FAFSA" uses income from the prior- prior year (PPY). While the DRT has been available for several years, many families were not able to take advantage of the tool in the past because their prior year tax returns were not yet processed when they completed the FAFSA. However, the implementation of PPY expanded the ability for more applicants to use the DRT this year, since the vast

[4] http://edworkforce.house.gov/news/documentsingle.aspx?DocumentID=401466
[5]https://oversight.house.gov/wp-content/uploads/2017/03/2017-03-16-OGR-EW-to-DeVos-ED-DRT-Incident-due-3-30-.pdf
[6]https://oversight.house.gov/wp-content/uploads/2017/03/2017-03-16-OGR-EW-to-Koskinen-IRS-DRT-Incident-due-3-30-.pdf
[7]https://www.ed.gov/news/press-releases/update-internal-revenue-service-irs-and-federal-student-aid-fsa-statement-irs-data-retrieval-tool-drt
[8]https://ifap.ed.gov/dpcletters/GEN1704.html

majority of families had filed their prior- prior year tax returns almost six months prior to the date the 2017-18 FAFSA became available. Then, only a few months into the application cycle-- and close to many state and institutional scholarship deadlines-- the DRT was taken down, significantly diminishing the potential benefits of Early FAFSA and PPY.

The DRT not only simplified the FAFSA process for students and families, it increased the accuracy of their income data reported on the FAFSA. Because income data retrieved using the DRT are more accurate than self-reported data, ED has long publicized that applicants using the DRT are less likely to be selected for verification; further simplifying the application process, reducing delays in the awarding and disbursement of federal aid funds to needy students, and shifting the workload on financial aid office staff away from document collection and processing toward the more valuable task of counseling students. The DRT outage harms students and families in multiple ways, making the FAFSA more difficult to complete, making more students subject to verification, and leaving families with fewer available financial aid office resources for help navigating the financial aid process. A recent NASFAA survey of member institutions found that 55 percent of 192 respondents reported an increase in students selected for verification at their institutions since the DRT was disabled.[9] At one large, 4-year public alone, the percentage of applicants selected for verification increased by 60 percent following the loss of the DRT.

Further complicating matters, this processing cycle is unique due to the fact that both the 2016-17 and 2017-18 FAFSAs use the same income information from the 2015 calendar year. This creates the potential for conflicting information between the two award years (when applicants erroneously report income or tax information for a year other than 2015). ED flags the applicant's record if a conflict is significant and the institution must resolve the conflict before federal student aid can be disbursed. ED strongly urged use of the DRT to prevent the incidence of conflicting information and also offered the DRT as an option for resolving conflicts if applicants hadn't used the DRT upon initially completing the FAFSA. Now, with the DRT disabled, institutions are seeing a spike in conflicting information. Twenty-three percent of NASFAA's survey respondents indicated increases in records flagged for conflicting information since the DRT outage occurred. This means that more students and families must provide tax returns and other documentation to financial aid offices to establish eligibility for federal aid. Overall, 91 percent of survey respondents indicated that the DRT outage was negatively impacting their offices in some way.

[9] https://www.nasfaa.org/news-item/11883/Verification_Woes_Top_List_of_DRT_Concerns_in_Recent_NASFAA_Member_Poll

We also want to draw attention to the application and renewal processes for Income-Driven Repayment (IDR) plans, which also rely on the DRT. Borrowers enrolling in IDR plans are experiencing financial hardship. This hardship may be sudden, resulting from unforeseen events such as job loss or death of a wage-earning family member. Prompt enrollment in IDR plans is critical to the financial well-being of these borrowers as well as to keeping these loans out of default. The DRT was an effective way to ensure these borrowers got the relief they needed when they needed it. For borrowers experiencing longer-term hardship, re-enrollment in IDR plans is required annually. The DRT kept the re-enrollment process simple and expedient, ensuring continuity in IDR enrollment for qualified borrowers.

We understand that legitimate security concerns cited by ED and the IRS led to the tool being disabled. However, we are looking for an explanation of why users of the tool and other key stakeholders were not informed of this outage until nearly a week after the system went down. It is also unclear why federal agencies took no action to correct these issues if vulnerabilities were identified months previously.

The FAFSA continued to direct students to the DRT for some time after the tool's outage. Because the design of DRT directed students from the fafsa.ed.gov website to a separate IRS webpage, the effect was to kick students out of the FAFSA application before it was completed. Many students may have erroneously believed they had completed the FAFSA or have simply given up, thinking they weren't eligible for aid or that the process was too complicated. The lack of communication and update to the FAFSA website is unacceptable, and caused quite a bit of strain, especially in the middle of the financial aid application season.

The DRT is an essential tool for students and families navigating the complex system of applying for federal student financial aid. Its benefits go beyond simplifying and shortening the application process for applicants; importing data directly from the IRS into the FAFSA also ensures data accuracy, preserving program integrity of the federal student aid programs. The abrupt shutdown of the DRT with no advance notice to stakeholders, no public acknowledgment for nearly a week following the outage, and the delay in updating federal student aid websites, including the FAFSA site itself, all caused unnecessary confusion, anxiety, and stress for students at an already-stressful time that coincided with many state and institutional financial aid application deadlines.

While the IRS was able to identify 100,000 individuals impacted by the data theft, it may not be possible to measure the impact of the DRT outage on students who may have missed a financial aid deadline or never even completed a financial aid application because of this issue, and whose college plans may have been compromised as a

result. Perhaps most troubling is the fact that this situation could have been avoided with better decision making in September, 2016, when the potential for abuse of the DRT was first identified[10].

The IRS and ED could have been working to implement security enhancements for the past six months that would have prevented not only the DRT outage but also the fraudulent activity ultimately identified in March, 2017. Timely restoration of the DRT is essential, as is a firm deadline by which the tool will be available again. If the tool is reactivated with additional authentication steps for students, we ask that ED consider the implications of a more complicated process on low-income families. Finally, any new front-end changes should be informed by stakeholder input, to ensure that the DRT continues to serve as a cornerstone for FAFSA simplification efforts.

[10]https://www.washingtonpost.com/news/grade-point/wp/2017/04/06/identity-thieves-may-have-hacked-files-of-up-to-100000-financial-aid-applicants/?utm_term=.99d84b4becd5

Statement to U.S. House of Representatives
Full House Committee on Oversight and Government Reform
"Reviewing the FAFSA Data Breach" Hearing (May 3, 2017)
Comments from National College Access Network

Chairman Chaffetz, Ranking Member Cummings and members of the Committee, thank you for this opportunity for the National College Access Network (NCAN) to submit comments for the record in advance of your May 3, 2017 hearing "Reviewing the FAFSA Data Breach."

NCAN's mission is to build, strengthen, and empower communities committed to college access and success so that all students, especially those underrepresented in postsecondary education, can achieve their educational dreams. As part of our efforts to help low-income students to and through college, we dedicate significant time and resources to helping students and families complete the Free Application for Federal Student Aid (FAFSA) to access federal student aid – including Pell Grants, Federal Work-Study and Direct Loans – that makes their college enrollment and completion possible and affordable.

We submit these comments to give you a picture of what the IRS Data Retrieval Tool (DRT) outage has meant to students and families across America, as well as the larger picture of college-going in our country and support for an educated workforce for a competitive America. This issue has wide impact, affecting not only prospective and current college-going students of all ages, but also other stakeholders such as colleges and universities, state aid agencies, private scholarship programs, school counselors, and community-based organizations supporting college access and success.

The DRT was instituted in 2009 as a way for FAFSA filers to access their tax filings and then import them into specific fields on the FAFSA's income questions. This innovation was used by 37 percent of filers in the 2015-16 cycle, allowing them to ensure the accuracy of their FAFSA with verified data, and complete the FAFSA faster with no need to find and manually type in figures from their tax returns. The DRT generally made the process more efficient by leveraging data already collected by another federal agency.

On March 3, 2017, at the height of the FAFSA submission cycle, just days before state deadlines fell in Indiana and Texas and a popular March 15 priority aid deadline fell at colleges and

universities across the country, FAFSA filers began receiving an error message when attempting to use the DRT function. When attempting to import their tax data using the DRT, filers were prevented from doing so and informed that "This service will be unavailable due to system maintenance." Yet at the same time, the FAFSA home page "announcements" still encouraged students to use the DRT. Further, within the online application, the link to the DRT remained live and continued to redirect students to the error message, from which they could not easily return to their FAFSA in progress. Frustrated applicants were not officially notified of the outage until almost a week later on March 9, when we learned the DRT would not return for "several weeks." The link to the DRT remained live for the next three weeks, until a modified announcement on March 30 said the DRT would not be available until the "start of next FAFSA season." (The 2018-19 cycle begins Oct. 1, 2017). It was the day after this second announcement on March 31 that the DRT link was finally removed from the FAFSA.

We share these quotes from on-the-ground stakeholders helping students respond to this outage:

The absence of this tool could lead to delays and roadblocks for filers. There is no indication about whether or when it will be back online. This new hurdle could not come at a worse time for young people entering college or continuing their studies. It imposes yet another barrier for students who already face multiple challenges to pursuing a college education and improving their lives. Unless corrected, this short-sighted action will negatively affect the prospects of promising young men and women in our community and across the country.
-- Robin Christenson, executive director, Capital Region Sponsor-A-Scholar, Albany, in an Albany Times Union letter to the editor (March 26, 2017).

Well, now due to the #IRSDRT outage, what happens is almost certainly verification. @FAFSA once eliminated barriers, now builds them.
-- Faith Sandler, executive director of the Scholarship Foundation of St. Louis in Missouri, in a tweet (March 23, 2017).

DRT was significantly better and less error prone. Can't believe they're not planning to bring it back before the next FAFSA filing cycle. Part of the problem/burden comes from our ability to complete verification ... but the bigger issue is the added burden this year of clearing the C399 codes. This is a particularly bad year to lose the DRT.
– Financial aid director at a public institution, in an email to NCAN (April 28, 2017).

"Literally every day that goes by, you have a chance of not getting aid you're eligible for."
– Austin Buchan, CEO of College Forward in Austin, TX, quoted in Inside Higher Ed (April 10, 2017).

"We want some real answers. We want some real action to start taking place so these kids can get what they need."

– Cheryl Jones, program director of the Access College Foundation in Norfolk, VA, quoted in Inside Higher Ed (April 10, 2017).

"If that language is still on the colleges' and universities' verification documents, it creates more confusion."
– Ann Hendrick, director of Get2College in Mississippi, told Inside Higher Ed that some colleges are sending FAFSA applicants verification notices that still advise them to use the DRT to address verification issues.

We cannot afford any more down time in this process; equity, access, and opportunity are at stake.
– Faith Sandler, executive director of the Scholarship Foundation of St. Louis in Missouri, in an email to NCAN (March 8, 2017).

NCAN members also detailed how the outage has prevented students from getting money for college. One saw his odds of receiving state grant aid fall as he waited for a tax transcript after being elected for verification, which could have been avoided had DRT been available to provide verified information. Another had his aid award package delayed an additional two weeks.

As these comments indicate, this is an emergency, not a mere inconvenience. We anticipate that approximately 10 million FAFSAs have yet to be filed this year, primarily from lower-income students who typically file later and renewing college students, community college students, and post-traditional students (older, attending part-time, etc.) who file closer to the start of classes.

We applaud the Committee for its attention to this urgent matter. We hope for a quick restoration of the tool in a way that strikes the delicate balance of data security and usability for the students and families seeking assistance in financing college. NCAN and its members stand at the ready to help design that solution and test it with users of the tool. Thank you again for this opportunity and please call on us moving forward.

Contact: Kim Cook, Executive Director, National College Access Network
(202) 347-484 x205, cook@collegeaccess.org

American Council on Education™
Leadership and Advocacy

One Dupont Circle NW
Washington, DC 20036
202 939 9300
acenet.edu

April 12, 2017

Secretary Betsy DeVos
United States Department of Education
400 Maryland Avenue, SW
Washington, D.C. 20202

Dear Secretary DeVos,

On behalf of the undersigned higher education organizations, we write to express our grave concern with the recent suspension of the Internal Revenue Service Data Retrieval Tool (or IRS-DRT). Subsequent announcements have indicated that the tool will not be available to student aid applicants for the remainder of this award year, and is not expected to be operative until October 1, 2017, at the earliest.

This extreme delay will have a profound impact on low-income students applying (or reapplying) for federal financial aid and borrowers applying for income-based repayment plans. The consequences of suspending the DRT undermine the benefits of the recent shift to using Prior-Prior Year income and tax data. We have already seen the negative impact of the loss of this tool, as students and families have experienced unnecessary confusion and states have been forced to delay application deadlines, all leading to more barriers to college for low income and other students. Furthermore, as many states base their state aid programs on federal eligibility determinations, complications with filling out the Free Application for Federal Student Aid will necessarily introduce additional delay and difficulty for students.

We recognize the seriousness of the IRS' concerns regarding the security of data and the possible misuse of the tool to commit tax fraud, but this should not preclude the timely adoption of reasonable security measures or a revised system. Use of the IRS-DRT is not merely a convenience to students: it is vital to ensuring that students, particularly those least likely to receive federal financial aid, can in fact do so.

We urge Department of Education and the Internal Revenue Service to use all necessary resources to resolve these issues as quickly as possible. In the meantime, we request that the Department take immediate steps to alleviate the increased burden that is now falling on millions of student applicants.

Our organizations and our members are eager to work with you to quickly restore this critical tool and guarantee that students and their families are able to reliably access the federal financial aid programs you oversee.

Sincerely,

Molly Corbett Broad

Internal Revenue Service Data Retrieval Tool
April 12, 2017

On behalf of:

ACPA - College Student Educators International
American Association of Colleges of Nursing
American Association of Collegiate Registrars and Admissions Officers
American Association of Community Colleges
American Association of State Colleges and Universities
American Council on Education
American Dental Education Association
Association of American Universities
Association of American Medical Colleges
Association of Catholic Colleges and Universities
Association of Community College Trustees
Association of Governing Boards of Universities and Colleges
Association of Jesuit Colleges and Universities
Association of Public and Land-grant Universities
Association of Research Libraries
Council for Christian Colleges and Universities
Council for Opportunity in Education
Educational Testing Service
EDUCAUSE
Hispanic Association of Colleges and Universities
NASPA - Student Affairs Administrators in Higher Education
National Association of Independent Colleges and Universities
National Association for College Admission Counseling
National Association of College and University Business Officers
Thurgood Marshall College Fund
University Professional and Continuing Education Association

epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

May 2, 2017

The Honorable Jason Chaffetz, Chairman
The Honorable Elijah Cummings, Ranking Member
House Committee on Oversight and Government Reform
2157 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Chaffetz and Ranking Member Cummings:

We write to you regarding the upcoming hearing on "Reviewing the FAFSA Data Breach."[1] We thank you for your interest in this issue and urge you to support a Student Privacy Bill of Rights. American students face unprecedented privacy and security threats. The increasing commercialization of personal data has led to staggering increases in identity theft, security breaches, and financial fraud in the United States. The Department of Education collects extremely sensitive personal information such as Social Security Numbers, and has an obligation to protect that data, but has failed to do so.

EPIC is a public-interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC is a leading advocate for student privacy rights.[2] EPIC has proposed a Student Privacy Bill of Rights to safeguard student data and security,[3] obtained documents regarding the misuse of education records through the Freedom of Information Act, and repeatedly urged the Federal Trade Commission to establish security

[1] *Reviewing the FAFSA Data Breach*, 115th Cong. (2017), H. Comm. on Oversight and Gov't Reform, https://oversight.house.gov/hearing/reviewing-fafsa-data-breach/ (March 22, 2017).
[2] See, e.g., *Student Privacy*, EPIC, http://epic.org/privacy/student/; Letter from EPIC et al. to Secretary John B. King, U.S. Department of Education (June 6, 2016), https://epic.org/privacy/student/ED-Data-Security-Petition.pdf; Comments of EPIC to the Institute of Education Sciences and Department of Education, Privacy Act of 1974; System of Records—"Impact Evaluation of Data-Driven Instruction Professional Development for Teachers", Jan. 4, 2016, *available at* https://epic.org/privacy/student/EPIC-Comments-ED-Impact-Eval-SORN.pdf; Comments of EPIC to the Department of Education, Notice of New System of Records: "Study of Promising Features of Teacher Preparation Programs", Jul. 30, 2012, *available at* https://epic.org/privacy/student/EPIC-ED-SORN-Cmts.pdf; Comments of EPIC to the Department of Education, Family Educational Rights and Privacy Act Notice of Proposed Rulemaking, May 2, 2011, *available at* http://epic.org/privacy/student/EPIC_FERPA_Comments.pdf; The Privacy Coalition to Donald Rumsfeld, Secretary of Defense, DOD Database Campaign Coalition Letter (Oct. 18, 2005), *available at* http://privacycoalition.org/nododdatabase/letter.html; Br. *Amicus Curiae* Electronic Privacy Information Center Supp. Apl., *Chicago Tribune Co. v. Bd. of Trustees of Univ. of Illinois*, 680 F.3d 1001 (7th Cir. 2012) (No 11-2066), *available at* http://epic.org/amicus/tribune/EPIC_brief_Chi_Trib_final.pdf.
[3] EPIC, *Student Privacy Bill of Rights*, https://epic.org/privacy/student/bill-of-rights.html.

standards for student data maintained by state agencies.[4] EPIC also sued the Department of Education regarding changes in an agency regulation that diminished the safeguards set out in the Family Educational Rights and Privacy Act.[5] The practical consequence of the FERPA rule change was to make it easier for private parties to get access to sensitive student data.

The Department of Education has recognized that data security is an "essential part of complying with FERPA as violations of the law can occur due to weak or nonexistent data security protocols."[6] Yet, the Department "does not believe it is appropriate to regulate specific data security requirements under FERPA."[7] As a consequence, student data is routinely compromised "due to weak or nonexistent data security protocols."[8]

Here are a few examples[9] of weak or nonexistent data security protocols have led to the disclosure of education records in violation of FERPA:

- A University of Maryland database containing 287,580 student, faculty, staff, and personnel records was breached in 2014; the "breached records included name, Social Security number, date of birth, and University identification number." The records go as far back as 1992.[10]
- In 2015, computer criminals hacked the University of Berkeley's Financial System and gained access to Social Security numbers and bank account information for approximately 80,000 students, vendors, staff, and current and former faculty. By some estimates, the breach impacted "approximately 50 percent of current students and 65 percent of active employees."[11]
- Edmodo, the self-described "number one K-12 social learning network in the world" boasting "over 39 million teachers, students, and parents," previously collected student information over an unencrypted connection.[12]

---

[4] EPIC, *EPIC Uncovers Complaints from Education Department about Misuse of Education Records* (July 18, 2014), https://epic.org/2014/07/epic-uncovers-complaints-from.html.
[5] *EPIC v. U.S. Dep't of Educ.*, 48 F.Supp. 1 (D.D.C 2014).
[6] Family Educational Rights and Privacy Act Final Reg., 76 Fed. Reg. 75,604, 75,622 (Dec. 2, 2011).
[7] *Id.*
[8] *Id.*
[9] *See, e.g., Chronology of Data Breaches: Security Breaches 2005 – Present,* PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/data-breach (Select "EDU-Education Institutions); Benjamin Herold, *Danger Posed by Student-Data Breaches Prompts Action,* EDUCATION WEEK (Jan. 22, 2014), http://www.edweek.org/ew/articles/2014/01/22/18dataharm_ep.h33.html; Michael Alison Chandler, *Loudoun Schools Offer Details on Data Breach*, WASHINGTON POST (Jan. 8, 2014), http://www.washingtonpost.com/local/education/loudoun-schools-offer-details-on-data-breach/2014/01/08/d0163b50-78ad-11e3-8963-b4b654bcc9b2_story.html.
[10] UMD Data Breach, UNIVERSITY OF MARYLAND, http://www.umd.edu/datasecurity/.
[11] Janet Gilmore, *Campus Alerting 80,000 Individuals to Cyberattack*, BERKELEY NEWS (Feb. 26, 2016), http://news.berkeley.edu/2016/02/26/campus-alerting-80000-individuals-to-cyberattack/
[12] Natasha Singer, *Data Security Is a Classroom Worry, Too*, N.Y. TIMES, June 22, 2013, at BU1, *available at* http://www.nytimes.com/2013/06/23/business/data-security-is-a-classroom-worry-too.html.

The enactment of the Student Privacy Bill of Rights[13] should be a priority for this Congress. The Student Privacy Bill of Rights would provide students with the following rights:

1. **Access and Amendment:** Students have the right to access and amend their erroneous, misleading, or otherwise inappropriate records, regardless of who collects or maintains the information.
2. **Focused collection:** Students have the right to reasonably limit student data that companies and schools collect and retain.
3. **Respect for Context:** Students have the right to expect that companies and schools will collect, use, and disclose student information solely in ways that are compatible with the context in which students provide data.
4. **Security:** Students have the right to secure and responsible data practices.
5. **Transparency:** Students have the right to clear and accessible information privacy and security practices.
6. **Accountability:** Students should have the right to hold schools and private companies handling student data accountable for adhering to the Student Privacy Bill of Rights.

As school districts and companies that market services and products to students increasingly collect and use student data, the ability for students to have access to and control of that data will be increasingly important. Also important is the use of Privacy Enhancing Techniques (PETs) that minimize or eliminate the collection of personal information. [14]

Far more needs to be done to safeguard the personal information of students at American educational institutions.

We ask that this letter be entered in the hearing record. EPIC looks forward to working with the Committee on these issues of vital importance to the American public.

Sincerely,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Policy Director

[13] In 2015, President Obama rightly proposed legislation to safeguard student privacy. The Student Digital Privacy Act would have "prevent[ed] companies from selling student data to third parties for purposes unrelated to the educational mission and from engaging in targeted advertising to students based on data collected in school." Press Release, White House Office of the Press Secretary, Fact Sheet: Safeguarding American Consumers & Families (Jan. 12, 2015), http://www.whitehouse.gov/the-press-office/2015/01/12/fact-sheet-safeguarding-american-consumers-families.

[14] *See* Comments of EPIC, *On the Privacy and Security Implications of the Internet of Things*, FTC File No. ___ (June 1, 2013), https://epic.org/privacy/ftc/EPIC-FTC-IoT-Cmts.pdf.

Email Viewer

Message | Details | Attachments | Headers | Source

HTML

From: "webforms@hhws-www1.house.gov" <webforms@hhws-www1.house.gov>
Date: 4/21/2017 8:35:04 AM
To: "tn02ima@mail.house.gov" <tn02ima@mail.house.gov>
Cc:
Subject: IMA MAIL ON IRS Data Retrieval

SUBJECT: IRS Data Retrieval

MESSAGE:
The Honorable John J. Duncan JR:

As an acting financial aid administrator at Tennessee College of Applied Technology-Knoxville, I am writing to express my deep concern regarding the impact that the outage of the IRSâ€™s Data Retrieval Tool (DRT) is having on my studentsâ€™ ability to apply for and receive federal student aid. For nearly ten years, the DRT has allowed students to transfer their tax information directly into the Free Application of Federal Student Aid (FAFSA). The IRS DRT is the cornerstone of FAFSA simplification and the outage directly affects both the 2016-17 and 2017-18 award years and adversely affects low-income students. If not addressed by October 1, this will also affect 2018-19 applicants.

Along with the National Association of Student Financial Aid Administrators (NASFAA), I write to ask for your support in seeking relief for the millions of FAFSA filers who are, or will be, affected by the DRT outage. Students who are unable to use the DRT are more likely to be selected for verif ication an of ten arduous process that of ten delays the delivery of f inancial aid, and sometimes deters students f rom completing the f inancial aid process and attending college.

With a sincere desire to assist our students, in alignment with requests made by NASFAA and members of House and Senate education committees, I request that the Department of Education to provide the following relief for students:

1) Allow signed copies of federal tax returns from applicants to satisfy verification documentation requirements in place of DRT information and/or IRS tax return transcripts.

2) For tax non-filers, allow for the submission of W2 forms and allow applicants to note non-filing within the institutional verification worksheet.

3) Revise the verification selection criteria to provide a more generous tolerance to ensure that the numbers of students selected for verification remains stable and manageable by institutions so that financial aid processing can continue uninterrupted.

4) Provide an increase in the tolerance level before assigning an error (399) code that indicates a conflict in a students information between the 2016-17 and 2017-18 FAFSA.

Students and colleges in your district need the IRS to bring this tool back online as securely and quickly as possible. However, in the interim, these steps will go a long way toward helping students, particularly those with low income, access federal funding for postsecondary education.

Thank you for your time and consideration.

Sincerely,

Melissa A. Macko
Financial Aid
TCAT-Knoxville

Close

Responses from Mr. Matthew Sessa
Deputy Chief Operating Officer
Office of Federal Student Aid

Questions from Ranking Member Elijah E. Cummings

May 3, 2017, Hearing: "Reviewing the FAFSA Data Breach"

1. **In response to questions about the Department's ability to protect students from scams that are perpetrated against them by third parties with commercial interests in student loan accounts, former Chief Operating Officer James W. Runcie testified: "...we don't have any control over those entities." Please clarify your response by addressing the following related question:**

   Does the Office of Federal Student Aid have the authority to oversee the actions of third parties—including loan servicing companies—who engage in loan consolidation activities that are done in conjunction with student accounts? If so, what specific authority does FSA have?

   Federal Student Aid (FSA) contracts with several entities that serve as federal loan servicers to manage the servicing of millions of federal student loans. These federal loan servicers collect loan payments, advise borrowers about resources and benefits to better manage their federal student loan obligations, respond to customer service inquiries, and perform other administrative tasks associated with maintaining a loan on behalf of the U.S. Department of Education (the Department). Through this contractual relationship, FSA has authority to ensure that the actions of these federal loan servicers comply with the terms of their contracts.

   In contrast, the Department has no authority and jurisdiction over third-party so-called "debt relief" companies. State attorneys general, the Consumer Financial Protection Bureau, the Federal Trade Commission, and other agencies may have some limited authority and jurisdiction over these companies and their practices, especially as they relate to advertising and charging fees for services. The Department does not contract with "debt relief" companies which are in the business of lending money to make money or to charge borrowers fees to access programs that are available free of charge through their federal servicers. While some of these companies and organizations offer legitimate services to borrowers, others are simply looking to take advantage of borrowers. In recent years, some companies have employed sophisticated marketing tactics to target unsuspecting students, parents, borrowers, military service members, and their families. Such companies charge federal student loan borrowers for benefits that borrowers can receive for free from FSA's contracted federal loan servicers. Loan consolidation, income-driven repayment, loan deferments, forbearances, and forgiveness opportunities are among the free benefits that are available to federal student loan borrowers. Scam companies may convince unsuspecting borrowers to provide them with personal, sensitive information that permits the companies to access borrowers' accounts. In some cases, borrowers provide the companies with "power of attorney." In this way, these companies are able to "deliver" the services or benefits they market, while charging borrowers to do so. If these companies inappropriately use the Department's logo or other identifying information, including trademarks, to give the impression that they were working with or for the government, the Department can take action. Last year, for example, the Department sent cease and desist letters to two third-party "debt relief" companies that were using the Department's official seal without authorization.

   We routinely monitor feedback and complaints we receive from borrowers and others via the Federal Student Aid Feedback System to identify instances of "debt relief" companies inappropriately using our official seal and/or implying a relationship with the Department. When we identify such cases, we will work with the Department's Office of General Counsel—which, in turn, consults with the

Department of Justice—to determine if taking a cease and desist action is appropriate. In general, FSA does not prosecute cases against third-party "debt relief" companies engaging in unlawful behavior because the Department of Education does not have authority to do so. However, FSA weekly shares complaints of suspicious activity with the Federal Trade Commission's Consumer Sentinel System, an investigative cyber tool that provides members of the Consumer Sentinel Network with access to millions of consumer complaints. This data sharing occurs weekly. The Department is committed to making this information available to federal and state law enforcement agencies that have the authority to investigate potentially fraudulent claims by third-party "debt relief" companies.

The Consumer Financial Protection Bureau (CFPB) and the Federal Trade Commission (FTC) have independent jurisdiction, and both have separately taken enforcement actions against third-party debt relief companies in the past. Examples of actions taken by the CFPB include:

- https://www.consumerfinance.gov/about-us/newsroom/cfpb-takes-action-to-end-student-debt-relief-scams/
- http://files.consumerfinance.gov/f/201412_cfpb_complaint_the-college-education-services.pdf
- http://files.consumerfinance.gov/f/201510_cfpb_consent-order_the-college-education-services.pdf
- http://files.consumerfinance.gov/f/201412_cfpb_complaint_student-loan-processing.pdf

Examples of actions taken by the FTC include:

- https://www.ftc.gov/news-events/press-releases/2017/05/ftc-stops-operators-unlawful-student-debt-relief-credit-repair
- https://www.ftc.gov/system/files/documents/cases/strategic_student_solutions_complaint_0.pdf
- https://www.ftc.gov/news-events/press-releases/2016/02/ftc-brings-action-against-debt-relief-operation-targeted
- https://www.ftc.gov/system/files/documents/cases/160224studentloandirectcmpt.pdf

States also have jurisdiction over third-party "debt relief" companies, and some State attorneys general have taken action against such companies as well.

We have also encouraged institutions of higher education to be on the lookout for companies that inappropriately or without authorization state or imply that the company is working with a particular postsecondary institution to provide a benefit to student loan borrowers. Examples of such communication to institution include:

- https://ifap.ed.gov/eannouncements/121916ThirdPartyDebtReliefCoPhoneNumberDLServicingCtr.html
- https://ifap.ed.gov/eannouncements/033016ThirdPartydebtreliefcompaniesuseofinstitutionalnameslogosandothertrademar.html

We strongly recommend that institutions monitor whether there are organizations that are using the institution's name, mascots, logos, trademarks, or other identifying information in a manner that has not been authorized by the institution. If an institution believes that an organization is using, without the institution's approval, the institution's identity as part of its marketing efforts, we have recommended that the institution consider contacting its State's Attorney General's Office (or other state consumer protection agency) and/or consider taking legal action against the company. Further, we have elicited institutions' help to make sure their students understand that they do not need to pay

for loan benefits for federal student loans. We have implored institutions to warn their students, including on institutional websites, about so-called "debt relief" companies.

Despite FSA's customer education for borrowers, and outreach explaining that federal student loan servicers will consolidate federal student loans and provide a host of other services for free, as well as the fact that FSA has no affiliation with third-party so-called "debt relief" companies that charge fees, the efforts of the third-party "debt relief" companies can be effective. Consequently, FSA will continue to develop and broadly disseminate user education about these important topics and will look for ways to collaborate with others to better protect borrowers.

Additionally, FSA added language to the FSA ID terms and conditions and deployed language in the FSA ID and StudentLoans.gov log-in banners on May 14, 2017. This new language allows the Department's Office of Inspector General (OIG) to more effectively investigate and prosecute third parties that improperly create, access, or make changes to FSA ID accounts for commercial advantage or private financial gain. The 2018–19 online *Free Application for Federal Student Aid* (FAFSA® form) will deploy this banner Oct. 1, 2017. The banner implementation was in direct response to a recommendation in the OIG's September 2016 Management Information Report related to abuse by commercial third parties. The OIG, Department of Justice (DOJ), and United States Digital Service (USDS) advised FSA in the development of the banner language.

Responses from Mr. Matthew Sessa
Deputy Chief Operating Officer
Office of Federal Student Aid

Questions from Representative Stephen F. Lynch

May 3, 2017, Hearing: "Reviewing the FAFSA Data Breach"

1. **The IRS Data Retrieval Tool outage means that students seeking to enroll in an income-driven repayment plans, or attempting to annual rectify their income to remain in such plans, will have to do so manually rather than through the automatic link to their IRS data. As a result, there both students and student loan servicers will have to complete additional paperwork, and servicers will have to process applications manually.**

   a. **What guidance has the Office of Federal Student Aid (FSA) sent to servicers to better handle manual applications? Please provide copies of that guidance.**

      The IRS DRT was restored for the income-driven repayment (IDR) plan application on StudentLoans.gov on June 2, 2017. During the time the IRS DRT was unavailable to borrowers applying for an IDR plan, servicers were directed to refer to established processes and procedures for managing paper income documentation. While IRS DRT usage has grown over the years, a significant number of IDR applicants—roughly 17 percent in the year prior to the IRS DRT outage—have continued to document their income manually. In addition to mail and fax options, servicers had the capacity to receive income documentation electronically from borrowers prior to and throughout the IRS DRT outage. As a result, a robust process was already in place that could be scaled up to address the increased volume of manual submissions. FSA highlighted the availability of the electronic submission option in messaging to borrowers during the IRS DRT outage.

      FSA monitored servicer performance levels daily during the IRS DRT outage to ensure there were no negative impacts to borrowers, like long wait times or systemic failures by borrowers to recertify for an IDR. No such negative impacts were observed, and FSA continually provided guidance to servicers to apprise them of status updates throughout the situation (Attachment A).

   b. **How is FSA ensuring that borrowers are not harmed by servicing mistakes or errors as more applications are processed manually?**

      Because processes and procedures already existed for managing paper applications and paper income documentation, FSA directed servicers to refer to those processes and procedures during the IRS DRT outage. FSA monitored servicer performance levels daily to ensure that borrowers were not harmed. No such negative impacts were observed.

2. **According to a May 2, 2017, letter from the Consumer Financial Protection Bureau's Student Loan Ombudsman, the Data Retrieval tool outage revealed that, "[f]or certain borrowers, delays in IDR enrollment have a ripple effect that can amplify consumer harm."[1]**

[1] Letter from Seth Frotman, Student Loan Ombudsman, Consumer Financial Protection Bureau, to Persis Yu, Director Student Loan Borrower Assistance Project, National Consumer Law Center (May 2, 2017) (online at http://online.wsj.com/public/resources/documents/frotman.pdf).

a. Does FSA anticipate that the manual processing of applications will increase wait times for borrowers seeking to enroll in income-driven repayment plans or attempting to annual rectify their income as the result of the outage?

The IRS DRT was restored June 2, 2017, for the online IDR plan application. During the time the IRS DRT was unavailable, most servicers consistently did not exceed the 15-business day turnaround time for initial processing of IDR applications (new or recertification). FSA did see some slight increases in turnaround, but the levels remained within acceptable ranges. Only one of our nine servicers failed to consistently meet the 15-business day standard, in some cases seeing turnarounds of up to 20 days. FSA worked aggressively with this servicer to monitor performance and explore strategies, such as mandatory overtime, to improve turnaround times. All servicers are now within the 15-business day window.

On a daily basis, we reviewed and monitored the status of IDR applications, as well as servicers' processing and completion times. We also monitored the call stats; there was only a slight increase—less than one percent—in the call abandon rate and the average speed to answer (ASA).

b. Has FSA anticipated any change in loan servicer processing and behavior as a result of this outage? If so, how will guidance from the office address this?

Yes. Due to the potential increase in manual income documentation, FSA directed servicers to refer to established processes and procedures for managing paper income documentation and proactively contacted servicers to understand what strategies the servicers would enact to minimize processing delays during the IRS DRT outage. As needed, servicers reallocated resources and/or implemented overtime to minimize negative impacts to borrowers.

3. According to reports, the Department of Education has stopped issuing discharges under its borrower defense authority despite a growing backlog.[2] The Massachusetts Attorney General's Office has worked extensively with FSA and the Department's new Office of Enforcement to support student borrowers who have been victimized by predatory, for-profit schools. Under the last Administration, the Department announced that thousands of Massachusetts students from the Everest Institute (Corinthian Colleges) and the American Career Institute were eligible to have their loans discharged.

Is this true? When will the Department resume borrower defense discharges?

The processing of previously approved borrower defense discharges was paused temporarily while the Administration reviewed the prior work that was done and the decisions that were made. Processing of applications for discharges resumed in May, and final action on the previously approved discharges is proceeding. The Department is continuing to review additional discharge applications and will notify borrowers of the decision on their claims once those decisions are made.

For students who were notified of their borrower defense discharge in January 2017—including about 4,500 students who attended American Career Institute in Massachusetts—FSA stated in emails to these students that their discharges would be processed within 120 days of the January announcement, which would be around mid-May.

---

[2] *Feds Put Loan Forgiveness Program on Ice*, Politico Pro (Apr. 26, 2017) (online at www.politicopro.com/tipsheets/morning-education/2017/04/feds-put-loan-forgiveness-program-on-ice-022535).

a. Have these discharges been processed?

Fewer than 200 discharges for American Career Institute students remain to be processed.

b. If not, is the Department on track to deliver those previously announced discharges this month? If not, why not?

The processing of discharges for American Career Institute began in June and should be completed by mid-September.

c. When will those 4,500 defrauded Massachusetts students receive their promised federal student loan discharges?

We expect that that the students approved for discharge will receive their discharge in early September July.

Responses from Mr. Matthew Sessa
Deputy Chief Operating Officer
Office of Federal Student Aid

Questions from Representative Stacey E. Plaskett

May 3, 2017, Hearing: "Reviewing the FAFSA Data Breach"

1. **A September 26, 2016, Management Information Report issued by the Department of Education Office of Inspector General (OIG) found that "the FSA ID and the Personal Authentication Service (PAS) are being misused by commercial third parties to take over borrower accounts." The Inspector General's Special Agent in Charge confirmed in a transcribed interview with Committee staff on April 20, 2017, that companies with a "commercial interest" in student loan accounts were, in fact, "controlling thousands of accounts or creating thousands of accounts and controlling them."**

   At the hearing, I asked for "a list of the names of those companies that were doing that." In response to my question, former Chief Operating Officer James W. Runcie stated that the Office of Federal Student Aid could provide this information in "a month." Please provide the complete list of all companies involved in the activities that were the subject of the OIG's September 26, 2016, Management Information Report, as requested.

   The private commercial third parties involved in the activities that were the subject of the September 26, 2016, report by the U.S. Department of Education Office of the Inspector General (OIG) are wholly separate and distinct from federal student loan servicers that have a contractual relationship with Federal Student Aid (FSA). The commercial third parties that engage in the misuse of borrower accounts highlighted by the OIG have absolutely no relationship—contractual or otherwise—with FSA.

   These private commercial third parties offer to help borrowers with application processes, such as the Federal Direct Consolidation Loan application, for a fee. However, there is no application fee to consolidate federal student loans into a Direct Consolidation Loan. If a borrower contacts his or her federal loan servicer, the servicer can consolidate the borrower's loans for free through the established application process. Private commercial third parties are charging borrowers for assistance in this otherwise free application process. Often, private commercial third parties equate themselves to companies that prepare taxes for a fee.

   Given that FSA has no affiliation with, or oversight authority for, these private commercial third parties, it is difficult to know if the list of private student loan debt relief companies FSA maintains is complete. Additionally, many of these companies change names or merge with other related companies, adding to the challenge of knowing exactly who these companies are and where they operate with certainty. Attachment B represents a list of private commercial third parties that FSA maintains. Currently, FSA is determining the most effective way to accurately maintain and utilize the list in a way that protects FSA's customers' best interests. Inclusion on this list does not imply that the company engaged in the misuse that was the subject of the OIG's September 2016 report. The OIG would be the appropriate source for providing a list of the exact companies that engaged in the activity documented in the OIG's September 2016 report.

Responses from Mr. Matthew Sessa
Deputy Chief Operating Officer
Office of Federal Student Aid

Questions from Representative Robert C. "Bobby" Scott

May 3, 2017, Hearing: "Reviewing the FAFSA Data Breach"[1]

1. **I understand the need to protect tax data, but the unavailability of the Data Retrieval Tool (DRT) will likely increase the number of students asked to submit additional documentation to schools after Free Application for Federal Student Aid completion. Known as verification, this process adds additional burdens to students. In fact, in a recent survey, one in four financial aid administrators reported an increase in students selected for verification.**

   a. **Has the DRT outage led to an increase in students selected for verification, either overall or at certain schools?**

      Yes.

   b. **What data do you have to support this?**

      Between Oct. 1, 2016, and March 2, 2017 (before the IRS DRT outage), approximately 23 percent of *Free Application for Federal Student Aid* (FAFSA®) filers were selected for verification. Between March 3, 2017, and June 9, 2017 (during the IRS DRT outage and immediately following its restoration), approximately 33 percent of FAFSA filers were selected for verification, a 10-percentage point increase. In order to relieve schools of the increase in verification burden due to the unexpected IRS DRT outage, FSA implemented a reduction in the verification selection rate from 30 percent to 23 percent for the remainder of the 2017–18 FAFSA cycle.

      On April 24, 2017, the Department issued a Dear Colleague Letter extending flexibilities to postsecondary institutions that they may choose to use as part of their verification procedures. As indicated in the communication, in lieu of using the IRS DRT or obtaining an IRS transcript, institutions may consider a signed paper copy of the 2015 IRS tax return that was used by the tax filer for submission to the IRS as acceptable documentation to verify FAFSA/ISIR tax return information.

2. **We also know that federal student loan borrowers are affected by the DRT being down. In fact, 3.4 million borrowers had access to the DRT in the most recent year when applying for income-driven repayment (IDR) plans or updating their income information. While the DRT is down, borrowers with taxable income will have to use a paper application. Distressingly, some servicers are not providing borrowers with information about the outage or the necessary income documentation. And some servicers have failed to warn borrowers that due to the manual submission of the application, recertification may take longer than it has in the past.**

   If students enrolled in IDR miss their annual recertification deadlines, they will be placed in the standard repayment plan and will likely face unaffordable spikes in monthly payments—which increase their risk of delinquency and default—as well as interest capitalization, which can add substantial costs.

[1] By unanimous consent at the hearing, the Committee approved Rep. Scott's participation in the hearing.

While there are instructions on how to proceed without the DRT on the StudentLoans.gov site, it is simply not enough. Student loan borrowers have key consumer protections that can help mitigate the impact of servicing delays and breakdowns including providing alternative proof of income and a ten day grace period after a borrower's recertification deadline has passed.

a. What are servicers and the Department of Education doing to ensure that students know about these consumer protections?

Prior to the IRS DRT outage, FSA had processes and procedures established for servicers to follow related to the receipt of paper applications and income documentation. This prevented systemic servicing delays and breakdowns. As a standard practice, servicers begin reminding borrowers of their approaching IDR plan recertification deadline 90 days before the deadline and in regular increments thereafter. While FSA has worked diligently to help avoid any confusion or potential delays given the DRT outage, we so far have no evidence of borrowers missing deadlines due to the outage.

FSA communicated directly to borrowers, as well as to the media and financial aid stakeholders who support borrowers, about options available for providing alternative documentation of income. Communication and broad outreach included:

- Additional language about providing income documentation was added directly to the IDR online application and the application's confirmation page.

- FSA posts on Facebook and Twitter informed students, parents, and borrowers they can manually provide information, as well as sharing relevant IRS social posts about how borrowers can access their tax return information. FSA posts were shared widely by financial aid stakeholders, including college access professionals/mentors, counselors, and advocacy groups.

- The joint statements by the IRS and FSA included (1) information for students, parents, and borrowers that information can be provided manually and (2) instructions about how to obtain copies of tax information. All joint statement were posted in English and Spanish to StudentAid.gov—FSA's flagship information portal for students, parents, and borrowers—as well as to IFAP, the primary information portal for financial aid professionals. Announcements also were posted to the Financial Aid Toolkit, FSA's repository for resources and information for college access professionals, counselors, and mentors.

- Emails to more than 2,000 partner organizations and individuals reminded partners where students, parents, and borrowers can get the latest information about how to apply for federal financial aid without using the IRS DRT. Emails also informed partners of available resources for financial aid and college access professionals, counselors, and mentors.

b. Given what I can only assume will be an influx of paper applications, what is being done to ensure that servicers are prepared to handle this increase?

FSA has no evidence of an "influx of paper applications." The unavailability of the IRS DRT did not prevent borrowers from using the online IDR application altogether. Once the online application was submitted, borrowers were given the option to submit income documentation directly to the servicer electronically, by mail, or via fax. Servicers had the capacity to receive

income documentation electronically from borrowers before the IRS DRT outage. FSA, however, amplified the availability of this option in messaging to borrowers during the IRS DRT outage.

The IRS DRT was restored for the income-driven repayment (IDR) plan application on StudentLoans.gov on June 2, 2017. During the time the IRS DRT was unavailable to borrowers applying for an IDR plan, servicers were directed to refer to established processes and procedures for managing paper applications, as well as paper income documentation.

FSA monitored servicer performance levels daily during the IRS DRT outage to ensure there were no negative impacts to borrowers, like long wait times or systemic failures by borrowers to recertify for an IDR. No such negative impacts were observed, and FSA continually provided guidance to servicers to apprise them of status updates throughout the situation (Attachment A).

Responses from Mr. Jason Gray
Chief Information Officer
U.S. Department of Education
Questions from Chairman Jason Chaffetz

May 3, 2017, Hearing: "Reviewing the FAFSA Data Breach"

1. Does the Department consider misuse and or unauthorized access of FAFSA.gov to be a cybersecurity incident?

   a. Was the misuse and or unauthorized access of FAFSA.gov analyzed as a "major incident" distinct from the misuse [hack] of the IRS' Data Retrieval Tool (DRT)?
   b. If not, why not?

   The Department considers misuse and/or unauthorized access to its systems to be a cybersecurity incident. We did not, however, consider the access of FAFSA.gov by wrongdoers in conjunction with the DRT to be a "major incident" distinct from the incident involving the misuse of the IRS' Data Retrieval Tool (DRT) because there is no evidence that the malicious actors accessed any personal information held in the Department's systems. We believe this incident was a fraudulent scheme directed at retrieving tax data from the IRS. The malicious actors used stolen PII to start FAFSA forms in order to obtain information from the IRS so as to attempt to file fraudulent tax returns.

   We have, however, noted Congress' desire to be fully informed about cybersecurity matters, and we will inform the appropriate Committees of significant cybersecurity incidents, even if they do not meet the definition of a "major incident" under OMB 17-05. OMB 17-05 itself makes clear that nothing "preclude[s] an agency [from] reporting an incident or a breach to Congress that does not meet the threshold for a major incident." We are in the process of amending our incident response directive to meet the new requirements of OMB 17-12.

2. Do you believe the Office of Management and Budget's most recent definition of and guidance on (M-17-05) what constitutes a "major incident" is sufficient to analyze the DRT incident and how it impacts the Department?

   We believe that OMB M-17-05 is a significant improvement and clarification of prior OMB guidance on Federal information security and privacy requirements; however, there are instances as noted above that would require additional guidance or direction from OMB. Systems across the Federal Government interface with other Federal and third party systems to reduce undue burden to taxpayers and support their related missions. Future guidelines could be strengthened to include more detailed instructions on reporting requirements for interconnected systems.

3. Do you as the CIO have the necessary authorities over Federal Student's Aid (FSA) to be accountable for the data maintained on and accessible through its web applications - specifically FAFSA.gov?

As the CIO for the Department of Education, I take responsibility for all Department systems and the data that is maintained and accessed through those systems. However, the current organizational structure as it pertains to the IT workforce at FSA creates gaps in oversight and visibility that is required to fully understand and accurately report on the overall health of Department of ED systems. OCIO has made progress working with FSA and looks forward to continuing our efforts to mature our FITARA governance and oversight process.

4. Are there any administrative, regulatory, or bureaucratic barriers at the Department that inhibit your ability to secure the Department's networks and web applications?

   As addressed in question five, the Department is currently working within existing resources to recruit and sustain a top-tier IT workforce, which is critical to the development, deployment, and sustainment of the Department's networks and web applications.

5. How many IT professionals does the Department currently employ?
   The current number of Information Technology Specialists GS-2210 that work in the Department of ED is 249. Note there are additional Job Codes (GS-343 and GS-0510) that perform IT functions but are not classified as IT Professionals.

   a. How many of these employees have industry-recognized certifications?
      In December 2016, the Department submitted to Congress the Federal Cybersecurity Certification Assessment indicating that 49% of staff held appropriate industry-recognized certifications.

   b. Currently, how many openings does the Department have for IT or cybersecurity professionals?
      OCIO received a budgeted funding level to support 131 Full Time Employees in FY 2017. OCIO currently has 115 staff members on board and has received approval to hire 9.

   c. What is the greatest barrier to recruiting and maintaining a qualified IT workforce at the Department?
      The current hiring process takes at a minimum 80 days, which allows some qualified individuals to find other employment between applying for the vacancy and the final selection process. In addition, there is significant competition amongst other federal agencies and the private sector for qualified IT and cybersecurity staff. The Department often works at a disadvantage as the private sector and select Federal agencies may offer higher salaries and more attractive benefits to interested candidates.

Questions for the Record
May 3, 2017, hearing titled "Reviewing the FAFSA Data Breach" before the House Committee on Oversight and Government Reform

Questions for Mr. Kenneth C. Corbin, Deputy Commissioner, Wage and Investment Division

Questions from Representative Robert C. "Bobby" Scott

1. **By automatically populating income information, the IRS Data Retrieval Tool (DRT) helps two types of individuals: 1) students who are filling out their Free Application for Federal Student Aid (FAFSA) and 2) borrowers who are enrolling or re-enrolling in an income-driven (IDR) repayment plan.**

   According to the most recent data available through Federal Student Aid, more than eight million students apply for financial aid between April 1st and September 30th-the same timeframe that the DRT is expected to be unavailable. While many high school students have already submitted FAFSA applications, the DRT shutdown disproportionately affects community college students - many of whom are low-income and older students.

   Given that we are now past the deadline for individuals to file their tax returns, is there a way for the IRS to mitigate the risk of the vulnerability of the DRT in such a way that the tool could become available for use by FAFSA filers now until the encryption solution is deployed?

While we recognize the important role the DRT serves in helping students apply for financial aid and enroll in, or maintain eligibility for, income-driven repayment plans, protecting taxpayer information is our highest priority. We have been working closely with the Department of Education to safely return the DRT to service as soon as possible. Students and families should plan for the tool to be offline until the start of the next FAFSA season when extra security protections to the program can be added. However, we restored the IRS DRT for the income-driven repayment (IDR) plan application on StudentLoans.gov on June 2, 2017.

It should be noted that we explored the possibility of returning the DRT to service using alternate technical mitigations. We decided, however, that these mitigations would not sufficiently reduce the risk of fraud and would require resources that would otherwise be put toward the encryption solution.

While the DRT for FAFSA is unavailable, the FAFSA applications are still available and operable. The income information needed to complete the FAFSA can be found on a previously filed tax return. Applicants who have not retained a copy of their prior year tax return can obtain a transcript of their account using the Get Transcript application on

IRS.gov. When using Get Transcript Online, registered users will receive the transcript immediately. If using Get Transcript by Mail, it will take an average of 5-10 calendar days to receive the transcript.

2. **My understanding is that the IRS recently introduced strengthened authentication processes for its electronic "Get Transcript" application, which provides tax filers on-line access to key data from their tax returns. However, I have heard that successful authentication requires users to have a mortgage, a car loan, or a credit card, and a cell phone in their own name. These requirements seem to be a barrier for many users, especially from low-income families.**

In order to use Get Transcript, tax filers must successfully authenticate their identity through Secure Access. We designed the Secure Access e-authentication solution to comply with OMB Memorandum M-04-04[1] and National Institute of Standard and Technology (NIST) Special Publication 800-63r2[2] Level 3 assurance guidelines, which significantly increase the rigor to resolve the identity of a user as required for web applications requiring "High confidence in the asserted identity's validity" and requires multi-factor authentication techniques for web applications. In order to meet these guidelines, we incorporated financial verification into Secure Access e-authentication. The IRS considered several options, and determined that we could consistently confirm through record checks, account numbers for a credit card, home mortgage loan, home equity (or second mortgage) loan, home equity line of credit (HELOC), or car loan. A credit bureau provided a representative sample of its user population, which demonstrated that 80% had credit cards, 57% had auto loans, 68% had a mortgage, and 63% had a home equity loan. As a result, we determined that we could reasonably confirm the taxpayer identities while adhering to NIST guidance. We continue to look at ways of increasing access to our online tools for all taxpayers, including low-income individuals, while maintaining appropriate levels of security.

   a. **Can you please explain what families need to use the "Get Transcript" application?**

To use Get Transcript, tax filers must complete the Secure Access process. Although returning users can log in with an existing username and password and a security code sent by text to a mobile phone, new users need the following:

- An email address;
- Social Security number (SSN);
- Filing status and address from last-filed tax return;
- Personal account number from one of the following:
  - credit card,
  - home mortgage loan,
  - home equity (second mortgage) loan,

[1] Available at https://georgewbush-whitehouse.archives.gov/omb/memoranda/fy04/m04-04.pdf.
[2] Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf.

  - home equity line of credit (HELOC), or
  - car loan
- A U.S.-based mobile phone. The user's name must be associated with the mobile phone account.
- If applicable, temporary removal of a "credit freeze" on the user's credit records through Equifax.

We do not retain the user's financial account information.

To complete the process, new users must:
- Submit their name and email address to receive a confirmation code;
- Enter the emailed confirmation code;
- Provide SSN, date of birth, filing status, and address on the last filed tax return;
- Provide financial account information for verification from the above list;
- Enter a mobile phone number to receive a six-digit activation code via text message or request an activation code by mail;
- Enter the activation code; and
- Create a username and password, create a site phrase, and select a site image.

b. Do certain users, such as low income individuals, have a tougher time getting access?

We take seriously our responsibility to secure taxpayer data in order to protect taxpayers from identity theft and prevent cyber criminals from accessing government revenue through refunds.

Our demographic data analysis indicates that lower income taxpayers do not complete the Secure Access steps as often as taxpayers with higher income. This is in part because our security standards require financial verification, or a financial account, for identity verification. In order to increase broader access, the IRS provides two other options for a taxpayer to request and obtain a transcript: on the web by using Get Transcript by Mail, or via an automated self-service telephone application. Both options mail the transcript to the taxpayer's address of record. In this way, we ensure that taxpayers have multiple ways of obtaining their tax data through self-service options. We continue to look at ways of increasing access to our online tools for all taxpayers, including low-income individuals, while maintaining appropriate levels of security.

Questions for the Record
May 3, 2017, hearing titled "Reviewing the FAFSA Data Breach" before the House Committee on Oversight and Government Reform

Questions for Ms. Gina Garza, Chief Information Officer

Questions from Chairman Jason Chaffetz

1. **The written testimony of Deputy Inspector General Camus states that the "same individuals and groups engaging in criminal activity on the e-Authentication portal are involved in this exploit of the FAFSA and the DRT." When were you first made aware of the connection between the two hacks?**

In early March 2017, after detecting potentially criminal activity, the IRS and the Department of Education temporarily suspended access to the Federal Student Aid – Datashare (FSA-D) Data Retrieval Tool (DRT). We first learned about the potential connection between the criminal activity on the DRT and the e-Authentication portal when we received the written testimony from the Treasury Inspector General for Tax Administration (TIGTA) on May 2, 2017.

   a. **Do you agree with the IG's assessment?**

We have not yet concluded that the same perpetrators participated in the e-Authentication and DRT incidents. Our research indicates that perpetrators tried to file fraudulent returns using data they got from the DRT. Since we are still reviewing these returns, we cannot confirm that they are fraudulent.

2. **The written testimony of Deputy Inspector General Camus states that "In September 2016, TIGTA detected an attempted access to the AGI of a prominent individual. When we investigated the attempted access, we determined that the FAFSA application and the DRT were used in this attempt."**

   a. **Did you alert the "prominent individual" that their personally identifiable information had been compromised? If not, why not?**

In September 2016, our systems detected and prevented a perpetrator from accessing the Adjusted Gross Income (AGI) of a prominent individual using public or illegally obtained personally identifiable information. After analyzing the incident, we determined that the perpetrator did not get the taxpayer's personally identifiable information from IRS systems. Since we only notify taxpayers if their personally identifiable information has been compromised because of a system breach or we made an unauthorized disclosure, we did not alert the individual.

b. In the wake of the September 2016 incident involving the "prominent individual" did you identify the fraudulent pattern of use of the FAFSA or the DRT to the Department? If not, why not?

Based on our analysis, the September 2016 incident was an isolated attempt to gain access to the individual's tax information. We did not identify a fraudulent pattern. After the incident, we added safeguards for Social Security numbers of high-profile taxpayer accounts in order to mitigate the risk of unauthorized access to their tax information.

However, for the DRT overall, when we discovered the potential DRT vulnerability in September 2016, we took immediate action by increasing monitoring and blocking IP addresses as a short-term solution. By January 2017 we had started working with the Department of Education to analyze longer-term solutions, which required changes to both the DRT and to the Department of Education applications. We agreed with the Department of Education that since we did not have any confirmed criminal activity we would monitor the DRT application, rather than shut it down immediately and thereby burden students applying for financial aid. But we advised the Department of Education that if we noticed an indication of identity theft, we would shut down the application.

c. Was there ever any consideration to notify Congress and/or federal law enforcement that the "prominent individual's" personally identifiable information had been compromised?

Federal law enforcement (i.e., TIGTA) notified us of the unsuccessful attempted access. No personal taxpayer data for the "prominent individual" was compromised, exposed, or disclosed by IRS systems. TIGTA maintains jurisdiction over the criminal investigation of this matter. We understand that TIGTA is conducting an ongoing criminal investigation into this incident.

Questions for Ms. Gina Garza, Chief Information Officer

Questions from Representative Will Hurd

1. **The IRS dealt with Get Transcript in 2015 and the FAFSA incident this year. These incidents will occur in the future and will continue to hurt taxpayers and our ability to invest in critical services like our military and care for veterans. To help prevent future issues, is the IRS investing in proven commercial technology that can examine tax, cyber, and external data securely, quickly, and at scale? Or is it continuing to rely on in house systems that have failed in the past?**

Securing taxpayer services and associated data is one of our highest priorities. We have invested in the use of proven commercial technologies for the examination of tax, cyber, and external data to prevent and detect fraudulent activity, as well as worked with our partners at the US Digital Service, and will continue to do so. We have strengthened protection and detection for FSA and DRT, and are working on expanding coverage to all affected services.